A Duly Diligent Response to the Concerns of Muslim System Stakeholders

Zulfiqar Ahmad

A thesis submitted in partial fulfillment of the requirements for

Doctor of Philosophy in Computer Science

The University of Auckland

2011

Abstract

O my Lord, give me more of knowledge (Quran)

We develop the Quranic Rational Unified Process (QuRUP) by customising the Rational Unified Process (RUP). The QuRUP is developed to provide a duly diligent response to the Quranic concerns of Muslim system stakeholders. For a duly diligent response to the concerns of Muslim system stakeholders, software requirements must be harmonised with the Quran.

We demonstrate an application of the QuRUP by analysing Pakistan's Identity Management System (PIdM). By analysing the PIdM, we indicate applications of the QuRUP for harmonising a software system with the Quran. We focus our analysis on elicitation of Quranic privacy requirements in the PIdM. We find that the QuRUP can elicit important Quranic requirements which may be overlooked when the unmodified RUP is applied.

Acknowledgements

Which of your Lord's favors will you then deny? (Quran)

Bismillah al rahman al rahim (in the name of Allah, the most gracious, the most compassionate). I offer all the praises and gratitudes to Allah Subhana Wa Tala (glorified and exalted be He), the creator of all things and the Almighty, Who has bestowed upon me the quest for knowledge and granted me determination to accomplish this research.

I am wholeheartedly grateful to Prophet Muhammad (Sallallahu Alaihi wa Sallam), who advised the mankind to seek knowledge from the cradle to the grave. He is who taught us the words of Allah (the Quran) and he is the model for us to live in a society by completely submitting to the will of Allah.

My individual efforts were not sufficient for the accomplishment of this thesis Illa Beiznillah. Allah made several individual to help in my thesis. Help does not come only in the form of technical knowledge, but also through motivation, encouragement, time and support, and pertinent criticism which I have been given by many individuals.

I would like to thank to Dr. Fethi Ahmed, Mohsen al Attar, and Shaikh Rafat Najm

for your help to me in understanding the Quranic explanation that I used in this thesis. I would also like to acknowledge the efforts of Shaikh Rafat Najm which you performed in reviewing my thesis. I would also like to thank Prof. John Grundy and Dr. Ian Welch for your valuable suggestions on my PhD research work.

My special thanks go to Prof. Clark Thomborson, my supervisor, for the guidance, thought provoking suggestions, pertinent criticism, and encouragement that you provided me throughout this research. Your support in my study has been an invaluable asset for me. Your weekly research group discussion gave me an opportunity to learn what is research and it made me a research student. You not only taught me how to embark on a research problem but also taught me how to write correctly, precisely, and deductively. Thank you for being always next door to my lab whenever I was in need. I did not forget to acknowledge and offer thanks to Barbara Thomborson, for your help in structuring and editing my thesis. May Allah bless both of you with the wealth of Iman.

I thankfully acknowledge my fellow PhD students Bashir Hussain, Gul Shahzada Khan, Muhammad Amer Qureshi, Muhammad Naveed Zafar, Shafique Alam Burki, and other HEC scholars. I would also like to thank my friends Nek Zali Khan and Muhammad Zahid Hammad who are in Pakistan. The computer technical support by Muhammad Ibrahim Aalavi, Keith Johnston and Pan Hu can not be underestimated as well. Thank you all for sharing my struggles. I need to further thank Adil Ali, Dr. Yusuf Habib, and Muhammad Shaban Jokio for reminding and calling me for Zikr (remembrance of Allah).

I am, of course, particularly indebted to my parents, my brothers and sisters, and my wife for your monumental, unwavering support and encouragement on all fronts. Last but not least, I offer my regards and thanks to Higher Education Commission of Pakistan (HEC) on awarding me scholarship to do PhD.

Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

The ink of the scholar is more sacred than the blood of the martyr (Prophet Muhammad)

We propose the Quranic Rational Unified Process (QuRUP) to elicit Quranic requirements in software systems. Quranic requirements in software systems are statements which comply with the injunctions of the Quran. These requirements detail the concerns of Muslim system stakeholders. The QuRUP is our customised form of the Rational Unified Process (RUP).

The RUP is a well respected and widely used software development process (Kruchten, 2003; Zuser et al., 2005). The RUP is a use-case-driven process, which means that the use-cases defined in the initial phase of software development are the foundation for the rest of the RUP-based development process (Kruchten, 2003). To indicate the wide adoption of the RUP in software development, Kruchten (2003) mentions that leading companies which focus on telecommunications (Ericsson and Alcatel), manufacturing (Xeros and Intel), and system integrators (Oracle, Deloitte and Touche) use the RUP.

These companies use the RUP because software development best practices include requirement management, a significant part of the RUP. One of the benefits of effective requirements management is the satisfaction of important system stakeholders, which is a

strong indicator of system success (Kruchten, 2003; Zuser et al., 2005). Bahill and Henderson (2005) earmark the inappropriate response to the requirements of system stakeholders as one of the root causes of system failures. Improving the process of requirements elicitation will likely increase the chances of the success of the system. Oberg et al. (1998) emphasise the need for effective processes of eliciting and managing the requirements of system stakeholders.

> How can we improve the quality of the systems we build as our businesses, national economies, and daily activities become increasingly dependent on them? The answers, as always, lie in the people, tools, and processes applied to our profession. Requirements management is often proposed as a solution to the ongoing problems of software development, yet relatively little attention has been focused on improving the practice of this discipline (Oberg et al., 1998).

To reliably meet the concerns of system stakeholders, system developers must understand their concerns (Zuser et al., 2005). The concerns of stakeholders cannot be reliably met unless the system developers are aware of these concerns. The requirements of system stakeholders detail their concerns associated with the system (Obbink et al., 2001). By implication, we say that understanding or eliciting all important requirements of potential system stakeholders is an essential activity for the success of the system. Poor requirements elicitation will almost guarantee that the final project is a complete failure (Hickey and Davis, 2004). Elicitation of requirements in early stages of software development is generally considered vital.

While arguing in favour of early requirements elicitation during software development, Leffingwell and Widrig (2000) argue that the effort required to detect and repair an error during the requirements stage is significantly less than the effort required to detect and repair the error in later stages of software life-cycle. Jackson (1997) attributes imprecise requirements elicitation from system stakeholders as a major factor behind undesired behaviour of a system.

An important subset of system stakeholders is Muslim stakeholders. Muslims constitute around 24 percent of the world population, or approximately 1.65 billion people (Kettani,

2010). Kettani celebrates the fact that Muslims are a fast growing population of the world. Kettani expects Muslims will constitute one quarter of world population by 2020 and one third by 2075. Muslims want to avoid engagement in any system activity that contravenes the injunctions of the Quran; they want to be involved in systems which are harmonised to the injunctions of the Quran.

According to the Quran, *Allah* is the sole owner of the whole universe. In this thesis, the whole universe is a system. Defining further, by system we mean an entity that interacts with another entity, and every system is a subsystem of the universal system. A human being, a computer, and a food production machine are all examples of systems. Stakeholders of a system are also systems which influence the system or are influenced by the system.

Let us consider the example of the system which produces *Halal* foods. The Arabic word *Halal* means lawful or allowed. Its opposite is *Haraam* which means unlawful or prohibited. *Halal* food products are therefore those food products which are lawful for Muslims. The Quran specifies some general requirements for *Halal* foods. The stakeholders of a *Halal* food production system who are expert in the *Shariah* elicit the Quranic requirements for *Halal* foods.

Like *Halal* food production systems, Muslim stakeholders need their software systems to comply with the principles of the injunctions of the Quran. Unlike the case of a food production system which has some guidance in the Quran, for software systems we do find no explicit *Ahkam* in the Quran. We are now able to state the central question of our thesis:

> How can we respond appropriately to the Quranic concerns of Muslim stakeholders in software systems?

This question is of great importance to Muslims and for anyone who is developing systems with Muslim stakeholders. A failure to consult the Quran appropriately during system development is a failure to appropriately consider the needs of Muslims who will use this system. Of course it is possible that a system developer will inadvertently meet the needs of stakeholders who were not adequately consulted. However, it is more likely that these stakeholder needs will not be met; and indeed some evident failures have already occurred.

A prominent example of software systems that failed to meet the concerns of Muslim

stakeholders are the usual Internet search engines, *e. g.*, Google, Yahoo, and Ask. We are unaware of any evidence that the Quran was consulted during the development of these systems. Many Muslim parents, and indeed many non-Muslim parents, are "afraid that they, or their children, would bump into explicit [internet] content". Here we are quoting from an interview with Reza Sardeha, the Chief Executive Officer (CEO) of a company providing an internet search engine that was developed with input from an *Imam* (AlSaleh, 2009). This search engine won the best *Halal* innovation award at the World *Halal* Forum in Kuala Lumpur (Hussein, 2010). The filtering mechanism in ImHalal search engine was believed to allow Muslims to avoid surfing across any website that is not *Halal* (AlSaleh, 2009).

Maghaireh (2008) and Algarni (2010) stress the need to regulate software systems with the Quranic *Ahkam*. The essence of these two studies is the need to establish system compliance with the Quranic *Ahkam* such that Muslim system stakeholders' engagement in unlawful activities could be avoided.

Anir et al. (2008) and Norman et al. (2009) discuss the shortcomings of existing software systems to address the concerns of Muslims. Anir et al. (2008) argue the inadequacy of technology in Malaysia to reliably determine the *Halal* status of food products. As a result, Muslims consumed some unlawful food products which were incorrectly declared *Halal*. Norman et al. (2009) complain about the development of illicit systems in Malaysia to validate the *Halal* status of food products. The argument of Norman et al. (2009) that technological systems incorrectly declared some products as *Halal* implies that system developers were aware of the need of Muslims to have *Halal* foods but they could not fulfil this need in their developed system.

According to Norman et al. (2009), the development of illicit systems created confusion on the part of customers and consequently it badly affected the economy of *Halal* industry in Malaysia. Norman et al. (2009) insisted upon the development of a reliable software system to address the concerns of Muslims in determining the *Halal* status of food products.

The upshot of AlSaleh (2009); Anir et al. (2008); Norman et al. (2009); Maghaireh (2008); Algarni (2010) is the need to establish system compliance with the Quranic *Ahkam* so that Muslim system stakeholders' engagement in unlawful activities could be avoided.

These studies indicate the need to address the Quranic concerns of Muslim system stakeholders. The Quranic concerns of Muslim system stakeholders are their fears of involvement in unlawful activities and their desires of involvement in lawful activities.

Regarding system failures to address the concerns of Muslims, a more notable case is the failure of Facebook and Youtube. We analyse the failure of Facebook and Youtube and indicate the need of the QuRUP to appropriately address such failures to address the Quranic concerns of Muslim system stakeholders.

In 2010, Pakistani government blocked access from Pakistan to two software systems, Facebook and Youtube, because of their Islamically offensive contents (Zafar, 2010). According to an *Ulama* in Indonesia, Facebook itself should not be banned:

> ... it is merely a new communication medium created by human beings. "We just banned its usage if it is used excessively and could drive lust," [Muhammad Nabil Haroen] explained, citing an example on the usage of a knife, which could be positive or negative, depend[ing] on the user behind it (Aqsha and Begawan, 2009).

An Islamic jurist, however, points out that a system itself may be bounded.

> Telephone is an example of such a medium which is perfectly permissible, however, if the interaction is between two non-Mahram (strangers) then it will become impermissible. Similarly, if the medium of social interaction violates any Shari [Shariah] rules or make it extremely difficult to maintain them, then this medium will be impermissible [unlawful] as well (Desai, 2010).

We infer from this *Fatwa* that any software system that engages its Muslim stakeholders in unlawful activities would be an unlawful or *Haraam* system. The architecture or code of a software system is actually the backbone or the main controller of the software system. Therefore, among other factors, it is the code of software systems, which is computer understandable system requirements, that makes software systems lawful or unlawful. In other words, system requirements are important, at least technically, in defining system status as lawful because software code is written to achieve what system requirements specify.

The foregoing analysis suggests the importance of system requirements in establishing system states as *Haraam* or *Halal*. Therefore, improving Requirements engineering (RE) methodology is likely to improve system compliance with a law. Our conclusion, that an improved RE methodology or a duly diligent RE methodology is likely to improve system compliance, has significant implications for Facebook and Youtube. If the engineers of Facebook and YouTube knew a way to harmonise their system requirements and consequently the developed system with the Quran, without detracting from their design's usability, profitability, and suitability for use by non-Muslims, they'd quickly implement this harmonisation. This is because engineers of Facebook and YouTube do not want to be perceived as seducers who lure people towards unlawful system activities; they want their systems to be legal to use in Pakistan.

A duly diligent elicitation of Quranic requirements for Facebook and Youtube would be a worthwhile endeavour, because if the endeavour is successful it would lead to a significant improvement in these products. If the endeavour is unsuccessful then it would allow Facebook and YouTube to market their products more appropriately (I.e., only to non-Muslims).

The term due diligence and the importance to establish due diligence during RE are discussed in the rest of this chapter. We also discuss how due diligence can be achieved in software systems for the purpose of Quranic compliance.

The term "due diligence" is used for a number of concepts (Gole and Hilger, 2009). Davison and Fitzgerald (2010) also acknowledge the multiple usages of the term due diligence. Davison and Fitzgerald (2010) mention that the term due diligence is used to denote various concepts involving either the performance of an investigation of a business or person prior to signing a contract, or the performance of an act with a certain standard of care. According to the New Zealand Law Dictionary (2005), due diligence is "a close examination of a transaction and its related documentation".

We argue that dueness (relevant or what is expected) is determined from a source (*e. g.*, the constitution of a system, a legal book, an expert's opinion, a standard). The Oxford English Dictionary presents a similar notion of the word "due". According to the Oxford

English Dictionary, the term due means “of the proper quality” or in accordance with established rules. The person who establishes due diligence is a duly diligent person. To say it in another way, a person is duly diligent if he/she carefully performs an appropriate act. The carefulness of a duly diligent person is its diligence.

The commonly understood notion of due diligence is an investigation or a comprehensive analysis, often carried out by independent assessors, of a business system (Angwin, 2001). To accomplish an effective due diligence of a business system, Goforth and Goforth (2001) urge the need to analyse underlying technology of the business system. We argue that an analysis of a technological system to ascertain due diligence necessitates the need to establish due diligence during the development of the system. We note that Massey et al. (2010) are also of this opinion. Although Massey et al. (2010) did not say so directly, apparently they assume that the assessment of a system before signing a contract necessitates the development of the system with due diligence. For instance, they indicate that to demonstrate system compliance with a law, organisations must exercise due diligence in the development of system requirements.

Demonstrating compliance with a law is essentially evidence to an investigation or assessment of the system, and this assessment is conducted in a court of law (Breaux et al., 2006). In a separate study, Breaux et al. (2009) emphasised establishing due diligence in managing legal requirements during the development and operation of information systems. Organisations often need to demonstrate the evidence of due diligence for legal compliance of their developed software system (Breaux, 2009; Breaux et al., 2009). The requirement to establish due diligence from the RE stage suggests the need to develop a duly diligent RE process.

We are unaware of a documented duly diligent software development process which is earmarked to respond to the concerns of Muslim stakeholders of software systems. The RUP is likely to fail in identifying Quranic requirements unless its practitioners are extraordinary diligent in applying the RUP. In a diligent application of the RUP, its practitioners put special effort in eliciting the relevant use-cases, misuse cases, and other cases. Use and misuse cases are sufficient for a preliminary Quranic analysis but are insufficient for a

detailed Quranic analysis. A preliminary form of Quranic analysis should classify requirements into two categories: *Halal* and *Haraam*. To perform a detailed analysis, however, we must understand Quranic *Ahkam* (roughly translated as requirements). Quranic *Ahkam* cover five types of requirements. These five types are *Waajib* (obligations), *Haraam* (prohibitions), *Mandub* (recommendations), *Makruh* (deprecations), *Mubah* (free choices).

We develop the QuRUP, arguably a duly diligent process, to elicit Quranic requirements of Muslim system stakeholders. We define a duly diligent process as a well-defined set of appropriate tasks which certain roles accomplish (or follow) with diligence to discharge a duty or to perform an act. Kruchten (2003) defines a role as "the behaviour and responsibilities of an individual or of a group of individuals working together as a team". Kruchten (2003) further mentions that roles have tasks or activities; a task is a unit of work that an individual in that role may be asked to perform. By a well-defined set of tasks, we mean tasks which are ordered, have defined roles, have defined methods for roles to perform tasks, and have specified input and output artefacts.

We argue that the dueness in a duly diligent RE process is the appropriateness of its tasks to a source, and the diligence in it is the carefulness of its practitioners in applying the process. We think that a duly diligent RE process would entail high quality requirements. In this thesis, we assess the quality of a set of requirements by considering their completeness, consistency, correctness, prioritisation, and traceability. This list of quality attributes is broadly consistent with the quality attributes identified in academic writing on RE. We apply our notion of dueness in a RE process to describe the dueness of the QuRUP. We say that the dueness in the QuRUP is the appropriateness of its tasks to the Quran. The diligence in the QuRUP is the carefulness of its practitioners in applying it.

For an appropriate response to the concerns of Muslim system stakeholders, we work particularly on eliciting privacy requirements of Muslim stakeholders of software systems. For individual's privacy in software systems, we do not find any explicit *Ahkam* in the Quran. However, the Quran provides some *Ahkam* related to people's privacy in houses. To safeguard individual's privacy, the Quran also regulates people's communications with each other. One of the reasons behind modesty-related Quranic *Ahkam* is protection of people's privacy. We use the QuRUP to apply Quranic privacy-related *Ahkam* to software systems.

Essentially, we extend the Quranic privacy-related *Ahkam* which regulate a societal system to software systems.

We demonstrate our present work on the process of Quranic requirements elicitation using the QuRUP by analysing Pakistan's Identity Management System (PIdM). For this thesis, the PIdM is National Database and Registration Authority (NADRA). In the PIdM, We say NADRA is a data holder. Individuals whose personal information is collected by the data holder are data subjects. In Pakistan, this data holder, which is a government organisation, manages human's digital identities. To do this, NADRA issues a Computerised National Identity Card (CNIC) to individuals aged 18 years or more. The process of obtaining a CNIC and requirements on the stakeholders of the PIdM are discussed throughout this thesis.

In this thesis, we base our analysis of the Quran mainly on the Quranic explanation by Syed Abul Aala Maududi (Maududi, 1987), a contemporary Islamic scholar from Pakistan. In the Islamic world, Maududi's explanation of the Quran is considered an authoritative source of Quranic explanation. Our understanding of Maududi's explanation presented in this thesis is further reviewed for appropriateness by a Quranic expert, Shaikh Rafat Najm. Shaikh Rafat Najm studied law in *Jamia al-Azhar*, Egypt. Presently he is an *Imam* of the *Masjid* at Auckland University of Technology (AUT), New Zealand. In the following section, we indicate how opinions of Shaikh Rafat are used in this thesis. This section details our research methodology that we used to accomplish this research.

1.1 Research methodology

We accomplish our research in three steps. These three steps are identifying an important research question, proposing a solution to the research question, and validating whether the proposed solution appropriately solves the research question posed in step 1.

At page 3, we identify the research question of this thesis based on our examination of literature. The thesis question is how to respond appropriately to the Quranic concerns of Muslim stakeholders in software systems. We propose the QuRUP as an appropriate solution to the question. An appropriate solution to the question is to understand the concerns of Muslim system stakeholders and to develop a system such that the concerns of Muslim

system stakeholders are addressed in the developed system.

Understanding all the concerns of Muslim system stakeholders and then accordingly developing a system is beyond the scope of this thesis. This thesis goes only to the process of discovering Quranic privacy-related concerns of Muslims in software systems. Eliciting other types of Quranic requirements in addition to privacy requirements and developing a software system based on these requirements are two prime extensions to our work in response to the concerns of Muslim stakeholders of a software system.

To validate that the proposed solution appropriately solves the thesis question, we consider three ways. These three ways are assessment by a case study, validation by an area expert, and assessment of the QuRUP for due diligence. These three ways which constitute our evaluation criteria are discussed in Section 1.2. In Section 1.2, we also discuss some limitations of our evaluation criteria.

1.2 Evaluation criteria

We proposed the QuRUP as a duly diligent response to elicit the concerns of Muslim system stakeholders. To validate the applicability of the QuRUP, a case study of a software system is conducted to elicit requirements, using QuRUP, for the system. An Islamic scholar validated the appropriateness of the QuRUP to consult the Quran and the appropriateness of the results produced by applying QuRUP. The due diligence in the QuRUP is validated by examining the appropriateness of the QuRUP to consult the Quran and by assessing the output of the QuRUP for some quality attributes of requirements.

Assessment of requirements for quality attributes is often done to verify compliance of derived requirements to their corresponding legal requirements. Hassan and Logrippo (2008) earmarks completeness and consistency as two important aspects to be considered for compliance verification of derived requirements or enterprise requirements with their respective legal requirements. We evaluate the output of the QuRUP for quality attributes to validate due diligence established in the QuRUP. The appropriateness of our validation of the QuRUP for requirements quality attributes rests on our hypothesis that a duly diligent RE process would produce high quality requirements. In Section 1.2.1, 1.2.2, and 1.2.3, we further elaborate our evaluation criteria.

1.2.1 Assessment for due diligence

We argue that the QuRUP enables its practitioners to appropriately respond to the concerns of Muslim system stakeholders. Our argument has three steps. First we argue that an appropriate response to any situation has two important and necessary characteristics: one, that the response is due, *i. e.* relevant; and two, that the response is diligent, *i. e.* carefully performed. The second and third steps of our argument are to evaluate the dueness and the diligence of the QuRUP, in comparison to the RUP, for a situation requiring requirements elicitation from Muslim system stakeholders.

The diligence in the QuRUP depends upon the carefulness of its practitioners. We assume that the practitioners of the QuRUP would be diligent in applying the QuRUP to elicit Quranic requirements. The criteria that we use to evaluate the dueness of the QuRUP are its relevance to *Qiyas* and the attainment of high quality requirements by using the QuRUP.

1.2.1.1 Relevance to Qiyas

In the *Shariah*, *Qiyas* is an appropriate way to consult to the Quran in order to seek guidance from the Quran. We are unaware of any other method to consult the Quran to seek Quranic guidance for unregulated matters. It follows then RE processes which extract Quranic guidances must contain all tasks of *Qiyas*, or they must contain tasks equivalent to the tasks of *Qiyas*. We, therefore, evaluate the dueness of the QuRUP for its relevance to *Qiyas*.

To evaluate the QuRUP for its relevance to *Qiyas*, we compare its structure with the structure of *Qiyas*. The "structure of *Qiyas*" refers to the well-defined tasks of *Qiyas*. The structure of the QuRUP is the list and sequence of tasks, roles specified to accomplish these tasks, and methods to accomplish these tasks. In the comparison of the structure of *Qiyas* and the structure of the QuRUP, we determine whether or not each task of *Qiyas* is contained in the QuRUP. To justify the dueness of the QuRUP relative to the RUP, we compare the structure of the RUP with *Qiyas*. In this comparison, we examine whether or not each task of *Qiyas* is contained in the RUP.

In order to explain why we choose *Qiyas* to evaluate the dueness of the QuRUP, we first point out how the Quran and *Qiyas* are distinct to other regulations and methods to consult those regulations. When it comes to the topic of legal compliance, most of us

will readily agree that establishing compliance with one law is similar, in principle, to establishing compliance with another law. Where this agreement usually ends, however, is on the question of scope of regulations or commandments in various laws and disimilarity of methods to consult these laws.

Though the Quran is a regulation, the Quran is unlike any other regulations prevailing in the software industry. Unlike governmentally-imposed regulations, the Quran consists of the words of *Allah* in the Arabic language. Furthermore, the Quranic *Ahkam* are not intended to regulate any particular industrial system or software system. Instead, these *Ahkam* are general and regulate a societal system in all present and future contexts. Man-made regulations are usually focussed on specific types of systems. For example, the HIPAA regulations of the USA are focussed on health informatics systems, and are irrelevant to other types of systems. On the other hand, we do not see any direct focus of the Quranic *Ahkam* on software systems.

Not only the Quran is different to other regulations, the process of extracting requirements from Quran differs to how requirements for software systems are extracted from other regulations. Below, we summarise the approach to regulatory compliance described in Breaux and Antón (2008). This is a well-regarded and heavily-cited article. We then analyse how legal requirements elicitation for software systems in Breaux and Antón (2008) is similar and different to Quranic requirements elicitation for software systems.

To extract natural language legal requirements into formal predicates in first-order logic, Breaux and Antón (2008) developed and used four types of patterns. These four types of patterns are the basic activity patterns with modality, purposes, noun distinguished by verb phrases, and rules or conditions. In Breaux and Antón (2008), a software engineer applies these patterns to a legal text to generate rights and obligations.

In Breaux and Antón (2008), the basic activity pattern consists of four elements: subject, action, object, and modality. In the basic activity pattern, a subject performs an action on an object and modality distinguishes an activity as a right or an obligation.

The purpose pattern describes the reason of performing an action or the goal of an activity. The purpose is a constraint on an action, it is not a constraint on the actor who performs the action (Breaux and Antón, 2008).

The pattern to distinguish nouns from verb phrases is constructed by words like that, which, and who. These words are used in Breaux and Antón (2008) for cataphoric and anaphoric references. The rule pattern in Breaux and Antón (2008) describes the preconditions and postconditions (constraints) using condition keywords, e.g., if, unless, when, and except.

In applying the four patterns, Breaux and Antón (2008) first capture rights and obligations in legal texts by normative phrases. For instance, normative phrase "must permit", "must require", and "may not" represent obligations, whereas normative phrases like "has a right to", "may deny" and "retains the right to" represent rights. Then Breaux and Antón (2008) restate rights and obligations from legal texts into restricted natural language statements. Each restricted natural language statements is restricted to one discrete state or activity and it allows only one verb in it Breaux et al. (2006). In Breaux and Antón (2008), restricted natural language statements are mapped into semantic models or patterns that are amenable to formal analysis. By analyzing the elicited rights and obligations, a software engineer can further generate implied rights, obligations, and constraints.

The requirements elicitation process of Breaux and Antón (2008) is comparable to the process used in the *Shariah* to elicit Quranic requirements for software systems. In the *Shariah*, the process used to elicit Quranic requirements for software systems in *Qiyas*. We compare *Qiyas* with requirements elicitation process of Breaux and Antón (2008).

From the given patterns used in Breaux and Antón (2008), we note that the main construct in Breaux and Antón (2008) to capture a regulation is subject, object, action, the purpose of the action, and modality. A similar structure is used in *Qiyas* when a Quranic regulation is reasoned. However, Breaux and Antón (2008) and *Qiyas* differ in describing the purpose of an action. In Breaux and Antón (2008), the purpose is a high level goal that is achieved by the performance or nonperformance of an action. In Breaux and Antón (2008), the purpose of an action is determined by engineers. A similar concept in *Shariah* is *Hikmah* which describes the purpose of an action or inaction. In an application of *Qiyas*, the effective cause of an action is determined by an Islamic jurist (Moghul, 1991). The effective cause of an action is called *Illah*. Moghul (1991) mentions that *Hikmah* is effective

cause underneath *Illah* of an action. Sometimes *Hikmah* and *Illah* are used interchangeably. Even though according to Moghul (1991) and Kamali (1993), performing *Qiyas* on the basis of *Hikmah* is less reliable than performance of *Qiyas* on the basis of *Illah*. In the *Shariah*, determining *Illah* on an action is necessary for extending the ruling of the action. This suggests that the concept of purpose of an action in Breaux and Antón (2008) is not necessarily applicable to extracting requirements from the Quran.

In Breaux and Antón (2008), their requirements elicitation process is validated by determining the applicability of the process in the healthcare domain. Breaux and Antón (2008) conclude their process is valid because it generates requirements when applied in this domain. In Breaux and Antón (2008), we do not find any assessment of the steps of the and/or the output produced by using the process. Furthermore, the process developed by Breaux and Antón (2008) is applied by engineers therefore validity of the process depends upon the diligence exercised by the engineers. On the other hand, *Qiyas* is applied by a jurist who is expert in the *Shariah*. In extracting requirements from the Quran for a system, the jurist may seek assistance from an expert of the system.

In an application of *Qiyas*, an Islamic jurist ensures that *Qiyas*is applied correctly and correct output is generated. In the *Shariah*, *Qiyas* is recognized as an appropriate process to extract requirements from the Quran for matters that are not explicitly regulated in the Quran. Therefore, for centuries *Qiyas* is part of the *Shariah*. On the contrary, we are not aware of any recognition of Breaux and Antón (2008) in any legal system for capturing legal requirements for software systems.

In applying both Breaux and Antón (2008) and *Qiyas*, respective legal texts are consulted to identify different modalities. In Breaux and Antón (2008), modalities are identified by examining normative phrases in a legal text. Likewise, in an application of *Qiyas* modalities from the Quran are also indentified by examining normative phrases in the Quranic text. Examining normative phrases only in the Quranic text is insufficient to identify modalities. In addition to examining normative phrases, Islamic jurists analyse the Quranic text to identify modalities. Section 3.1 describes how modalities are identified by analyzing the Quranic text. In conclusion, then Breaux and Antón (2008) is inadequate to identify all Quranic modalities.

The differences of the Quran and *Qiyas* to other regulations and methods for extracting requirements from these regulations will not impede establishing Quranic compliance in RUP-based software development. For RUP-based development, IBM Rational (the current owner of the RUP) has listed commonly adopted regulations and standards with which software systems comply. In this list, the Quran is not mentioned, even though it is the standard regulation for Muslim stakeholders. The absence of the Quran from this list does not imply that in a RUP-based development, its practitioners will find it impossible to establish compliance with the Quran. Indeed, IBM leaves the legal compliance issue open to the practitioners of the RUP: "IBM customers are solely responsible for ensuring their own compliance with their legal requirements" (Wahli et al., 2006).

It is further mentioned in Wahli et al. (2006) that "It is also the customer's sole responsibility to obtain competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements". In this thesis, we argue that that Quranic compliance can be established in a RUP-based development; and we suggest one way (our QuRUP) in which this compliance can be performed with due diligence.

To validate the dueness of the QuRUP, we evaluate the the QuRUP for its relevance to *Qiyas*. To interpret the Quran for any particular system (*e. g.*, software systems), Muslim jurists adopt an established method, *i. e.*, *Qiyas* to consult the Quran. We are not aware of any other method closely similar to *Qiyas* which is used to interpret other regulations, nor we are aware of any approved method other than *Qiyas* to consult the Quran.

1.2.1.2 Attainment of high quality requirements

As we argued before, a duly diligent process is likely to produce high quality requirements. Common sense seems to dictate that a duly diligent QuRUP would enable its practitioners to attain high quality requirements. We evaluate the QuRUP for dueness by assessing the quality of requirements elicited through it. In this thesis, we assess the quality of a set of requirements by considering five quality attributes: completeness, consistency, correctness, prioritisation, and traceability.

Completeness, consistency, correctness, prioritisation, and traceability are quality attributes of requirements (Yilmaztürk, 2005). This list of quality attributes is broadly consistent with the quality attributes identified in academic writing on RE. Yilmaztürk (2005) reports that completeness, consistency, correctness, prioritisation, and traceability are among quality attributes that are commonly discussed by the academia and the industry.

By correct requirements, we mean error-free requirements. By consistency in requirements, we mean closeness in terminologies of software requirements and corresponding legal requirements. When terminologies of software requirements and legal terminologies closely match, it is easier to establish due diligence and legal compliance (Otto and Antón, 2007; Massey et al., 2008; Massey et al., 2010). Traceability is defined as the "ability to describe and follow the life of an artefact (requirements, code, tests, models, reports, plans, etc.) developed during the software life-cycle in both forward and backward directions" (Lucia et al., 2007). In the RUP, traceability of a requirement means to trace back the source of the requirement. Incomplete requirements are erroneous for a software system, so requirements elicited for a software system must be evaluated for completeness (Kamalrudin et al., 2010).

In the RUP it is recommended engineers obtain a prioritised, traceable, and valid set of requirements on the successful accomplishment of requirements elicitation activity. Requirements which are complete, correct, and consistent are valid requirements (Bahill and Henderson, 2005). Review meetings or follow-up sessions with stakeholders are ways of validating requirements (Paetsch et al., 2003). Along the same lines to the RUP, Massey et al. (2010) insist that certain concerns be addressed during RE. In software systems, three important concerns that must be addressed during RE are requirements prioritisation, traceability from legal texts to software requirements, and terminology mapping of software requirements to the corresponding requirements of a legal text (Massey et al., 2008; Massey et al., 2010). Likewise, Kamalrudin et al. (2010) indicate the importance of eliciting a complete set of consistent and correct requirements.

Yet another sober analysis on RE reveals that, in software systems, requirements adequacy, that is, their completeness, correctness, and consistency must be analysed (Adrion et al., 1982). In order to evaluate the QuRUP for attainment of quality attributes, we first

indicate how the QuRUP might be used to elicit a complete set of consistent, correct, prioritised and traceable requirements. Then we compare the QuRUP with the RUP for these quality attributes.

For completeness of requirements, we compare the requirements elicited through the QuRUP and through the RUP and check whether by using the QuRUP, any requirements is elicited that might have remained undiscovered in an RUP-based analysis of the PIdM.

To evaluate the QuRUP for consistency in requirements, we compare the terminologies of elicited requirements with the terminologies of their relevant *Ahkam*. The list of criteria we use to evaluate requirements consistency includes actor, action, data object, *Illah*, and *Hukm*. This list of criteria is an extension of the list of criteria specified in Massey et al. (2010) for terminology mapping. Massey et al. (2010) suggest actors, data objects, and actions for terminology mapping between requirements. Massey et al. (2010) state that actors are individuals which perform certain actions or tasks. Data objects are information elements mentioned either in software documentation or in a legal text with which compliance is achieved (Massey et al., 2010). The Arabic term *Illah* means effective cause and *Hukm* roughly means a requirement.

We evaluate the QuRUP for traceability of elicited requirements to their corresponding Quranic *Ahkam*. From the available documentation on the accomplishment of activities of the QuRUP, we find the traceability link between the software requirements and corresponding *Ahkam*. We also evaluate the QuRUP for prioritisation of requirements. To evaluate the QuRUP for prioritising requirements, we compare the criteria of prioritising requirements in a QuRUP-based analysis with a RUP-based analysis. Finally, we evaluate the QuRUP for correctness. In evaluating the QuRUP for correctness, we evaluate the correctness of elicited requirements and the correctness of our use of *Qiyas* for requirements elicitation.

1.2.2 Assessment by a case study

To validate the proposed process, we rely on an interpretive case study of the PIdM. Our aim in conducting this case study is to indicate the applicability of the proposed process, *i. e.* the QuRUP, can be applied to elicit requirements of Muslim system stakeholders, and to develop an understanding how an RE team would apply the QuRUP. In this case study,

our application of the QuRUP will remain on elicitation of Quranic-compliant privacy requirements of Muslim system stakeholders.

To explain how due diligence might be established by using the QuRUP, we indicate how *Sam* and *Qas* might use the Ahkamic diagram in the QuRUP to elicit requirements for the PIdM. The Ahkamic diagram is our extension of the UML use-case diagram. *Sam* and *Qas* are respectively system analyst and Quranic analyst of the PIdM. We assume that *Sam* is familiar with the privacy taxonomy of Solove (2006). We also assume that *Sam* has interacted with a data subject of the PIdM. A data subject is a human who has experience of interacting with the PIdM. Then we indicate how the QuRUP might be applied to the PIdM.

In order to apply the QuRUP, *Qas*, is added into the existing RE team of the PIdM. By using the QuRUP, *Sam* and *Qas* work together to elicit requirements for the PIdM. In the QuRUP, *Sam* elicits preliminary requirements and effective cause underneath each preliminary requirement. These preliminary requirements along with their effective causes are then given to *Qas*. On the basis of this input from *Sam*, *Qas* will then elicit Quranic requirements. We use the idealised scenario stated above to indicate how the QuRUP works. By using this scenario, we indicate an application of the QuRUP to the PIdM. In this application of the QuRUP, we elicit privacy requirements. These privacy requirements of the PIdM correspond to privacy-related Quranic *Ahkam*. In the application of the QuRUP to the PIdM, we assume that requirements of Muslim system stakeholder would not conflict with each other.

1.2.3 Validation by an expert

Our interpretive case study raised the need for a validation by a Quranic expert. In our research, Shaikh Rafat Najm validated the correctness of our consultation to the Quran in using the QuRUP and results produced. He also examined the QuRUP for its relevance to *Qiyas*. Lastly, he examined the elicited requirements to assess the quality of the requirements. His remarks are recorded in Chapter 6.

The interpretive case study to indicate the use of the QuRUP, validation by an Islamic scholar, and establishing due diligence for Quranic-compliance demonstrate the rigour of the research conducted in this thesis. However, we must admit the research conducted in this thesis still have some limitations. Below we discuss some limitations of our study, and

in Chapter 7 we will give recommendations how these limitations could be addressed in future work.

Appropriateness of the QuRUP for eliciting requirements from the Quran and appropriateness of the output artefact of the QuRUP are validated by an Islamic scholar and not by a jurist. In the *Shariah*, however, validation of an Islamic jurist is considered more powerful and appropriate over any validation done by an Islamic scholar. Likewise, the appropriateness of the Ahkamic diagram is validated by the Islamic scholar. In this study, the Ahkamic diagram is not validated at large scale for its communicativeness to system users.

The case study of this thesis is interpretive. This case study no doubt indicates how to apply the QuRUP, in a real application of the QuRUP the practitioners of the QuRUP may interpret the QuRUP differently. In an application of the QuRUP, its practitioners may not necessarily generate the same results to what we generated. Instead, they may generate entirely different requirements by using the QuRUP.

The case study of the PIdM is confined to eliciting privacy requirements only. The QuRUP is not tested to elicit another type of requirements. This does not mean that QuRUP can not be applied to elicit other types of requirements, *e. g.*, security or functional requirements. Instead, QuRUP can be applied to elicit other type of requirements from the Quran, because the process to consult the Quran is same for discovering any type of requirement. However, this thesis does not exhibit this explicitly.

This thesis does not deal with requirements of non-Muslims and their conflicts with Muslim system stakeholders. Moreover, in this thesis, it is assumed that requirements of Muslim system stakeholders would not conflict with each other. In reality requirements of Muslim system stakeholders could conflict with each. Addressing conflict between requirements of Muslims and conflict between requirements of Muslims and non-Muslim is an area of concern in a duly diligent software development process. This thesis provides some suggestions of ways to address this issue, but a complete resolution is beyond its scope.

The use of the privacy taxonomy of Solove (2006) as a part of the QuRUP is a limitation on the applicability of this process. We assumed that system analyst of the QuRUP is aware of Solove (2006) and will use Solove (2006); however, in a real application of the QuRUP

its analysts may not be aware of Solove (2006) or they may be required to use some other, possibly less US-centric, reference. Not using Solove (2006) in the QuRUP does not mean that QuRUP will fail if another referent for the word "privacy" is used, it is not unlikely then it will generate different results. Our use of Solove (2006) in our case study is thus a limitation on the validity of a more general QuRUP: one which does not rely on the analyst having knowledge of Solove (2006).

1.3 Contributions

This thesis presents five contributions. They are a customisation of the RUP for an appropriate response to the Quranic concerns of Muslims, an extension of UML use-case diagram to the Ahkamic diagram, a collection and categorisation of Quranic privacy-related Ahkam into Domestic-Communication-Modesty related Ahkam (DoCoMo), an identification of due diligence as an important goal of RE and a presentation of a method to establish due diligence for Quranic compliance during software development, and an integration of Quranic guidance on privacy with the US legal conception of privacy.

The main aim of this thesis is to address the question of how to respond appropriately to the concerns of Muslim system stakeholders. To respond appropriately to the concerns of Muslim system stakeholders, we customised a well known and widely used process, *i. e.* the RUP. The practitioners of the customised RUP can arguably respond appropriately to the Quranic concerns of Muslim in software systems. We believe that this contribution is novel because we do not find any process like the QuRUP which can be used to appropriately respond to the Quranic concerns of Muslims system stakeholders. We believe that both Muslim and non-Muslim system stakeholders are the potential beneficiaries of the QuRUP.

To communicate requirements to system stakeholders, requirements engineers often model preliminary requirements in an artefact which they present to system stakeholders. The UML use-case diagram is a well known artefact widely used in software engineering processes including the RUP. We find this artefact inappropriate to communicate Quranic requirements to Muslim system stakeholders. We extend this artefact to the Ahkamic diagram. We believe that the Ahkamic diagram is an appropriate and effective tool for requirements engineers to communicate requirements with Muslim stakeholders.

In an application of the QuRUP, we elicited privacy requirements for the PIdM. To elicit a requirement by using the QuRUP, there is a requirement to identify a relevant *Hukm* in the Quran. We analyse the Quran to its find privacy-related *Ahkam*. We synthesise these *Ahkam* into DoCoMo. We do not use all *Ahkam* of DoCoMo in the application of the QuRUP on the PIdM. However, for any reader who wants to know about privacy-related Quranic *Ahkam*, we hope our review of DoCoMo will serve the purpose. Our synthesis of privacy *Ahkam* might be helpful for readers for their comprehension and analysis of these *Ahkam*.

The due diligence is an important and well known concept in business. As far as our literature review guides us, a paucity of research studies suggests the need to establish this important concept in software engineering. This paucity indicates that this concept is relatively less known and less used in software engineering. We do not argue that the developers and the practitioners of RE processes can not be duly diligent in their practices to develop software systems; however, we are unaware of any RE process which explicitly requires or recommends to use the concept of due diligence during RE. To indicate how due diligence can be established in software development, we incorporate this concept in the QuRUP. We devised a list of criteria to evaluate due diligence in systems which are aimed to meet the Quranic concerns.

1.4 Structure of this thesis

This thesis is organised into a literature review, Quranic privacy concerns, and customisation the RUP into the QuRUP. In Chapter 2, we survey published literature related to stakeholder requirements elicitation. From this literature, we evaluate various requirements elicitation methods for their potential to respond Quranic *Ahkam* which specify requirements of Muslim stakeholders. In Chapter 3, we capture Quranic *Ahkam* related to people's privacy and review *Qiyas* for its use in extending these *Ahkam* to specify requirements in software systems. In Chapter 4, we customise the RUP to elicit requirements of Muslim stakeholders of software systems. In Chapter 5, we use the QuRUP, a customised version of the RUP, to elicit privacy requirements of Muslim stakeholders of the PIdM . In Chapter 6, we evaluate the QuRUP for a duly diligent response to the concerns of Muslim system stakeholders. In Chapter 7, we conclude our work by summarising our answer for

addressing the Quranic concerns of Muslim system stakeholders.

CHAPTER 2

Requirements Elicitation

Seek knowledge and wisdom, or whatever the vessel from which it flows, you will never be the loser (Prophet Muhammad)

Stakeholder requirements are among the most important artefacts in a software system. In system development, it is important to understand how requirements could be elicited and represented (Goguen, 1996). For a successful system, it is necessary to understand and meet the requirements of the potential system stakeholders. Muslims are a subset of potential stakeholders of software systems. In order to respond appropriately to the concerns of Muslim stakeholders of software systems, system engineers need to understand and meet the requirements of Muslim system stakeholders. To understand the requirements of Muslim system stakeholders, system engineers must elicit these requirements. Therefore, to elicit the requirements of Muslim system stakeholders, we customise the RUP to QuRUP.

To meet the requirements of system stakeholders, system developers' reliance on software processes is often helpful. In fact, effective software processes are critical to the success of organisations who develop and use software systems (Ambler et al., 2005). Lehman (1991) considers the software development process as the key to the development of satisfactory software. Lehman (1991) reminds us that an effective software development process is essential for economic and physical survival of the modern computer-dependent

society.

A process is essentially a systemic approach to the creation of a product or the accomplishment of a task (Osterweil, 1987). It defines who does what, when, and how (Kruchten, 2003; Fayad, 1997). In the terminology of the RUP, a process is defined as "a set of partially ordered work descriptions intended to reach a higher development goal, such as the release of a specific software" (Rational Software Corporation, 2005). A system development process such as the RUP guides project teams in producing high quality systems which meet the needs of their stakeholders (Ambler et al., 2005; Kruchten, 2003). Due to the wide adoption of the RUP in the software industry, it is considered a de facto standard process for software development, and arguably, the RUP can be considered an asset of software system-based organisations.

The RUP is a system development process originally developed at Rational Software. The RUP is not only a software development process, it is also a framework or methodology for system development which can be tailored by an organisation to meet their needs. In other words, it provides a structure from which development processes can be instantiated. IBM Rational also advocates that organisations may customise the RUP to create processes which meet their organisational needs. The Enterprise Unified Process (EUP) is an example of customising the RUP. The EUP customises the RUP by adding several new phases and disciplines to it (Ambler et al., 2005). The Essential Unified Process (EssUP) and the Agile Unified Process (AUP) are two other customisations of the RUP. In our customisation of the RUP to QuRUP, we chiefly concentrate on the requirements elicitation part of the RUP. This thesis uses the terms "requirements", "needs", and "requests" interchangeably.

The rest of the chapter is organised as follows. In Section 1, we introduce some basic concepts used in this thesis. In Section 2, we provide an overview of requirements elicitation activity of the RUP. In Section 3, we provide a short description of some commonly used requirements elicitation techniques and indicate the use of scenarios for eliciting requirements. In Section 4, we explain Ahkamic diagrams used in eliciting and communicating Quranic requirements. Section 5 concludes this chapter by summarising the work of this chapter and provides a brief description of the following chapters.

2.1 Preliminary concepts and definitions

In this section, we define and explain some basic terms and concepts used in this thesis. These are Islamic consideration of the QuRUP, our notion of a system for this thesis, system requirements, system stakeholders, and types of system requirements.

2.1.1 Shariah

The Arabic word *Shariah* means "path", or "path to water" or "path to a water hole". In Islamic jurisprudence, the *Shariah* is the path on which every Muslim should run. Islamic jurists consider *Masalih-al-Ibad* as the objective behind the *Shariah*. *Masalih-al-Ibad* means securing benefit and preventing harm for humanity. In the *Shariah*, regulations provided for *Masalih-al-Ibad* can be divided into the five Ahkamic categories: *Waajib*, *Haraam*, *Mandub*, *Makruh*, and *Mubah*. The two main sources for these *Ahkam* are the Quran and the *Sunnah*. *Sunnah* covers the traditions of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*). In the English language, the *Shariah* is roughly translated as Islamic law (Lombardi and Brown, 2006).

In Judaism, Halakha (also spelled Halaka) is an equivalent to *Shariah*. Halakha is translated as "the path" or "the way of walking". This term is used to denote the collective body of Jewish religious law. Some Jewish groups use internet and software systems by making them kosher (Čejka, 2009). They make these systems kosher by using them for religiously permitted purposes. To avoid viewing forbidden web-page content such as pornography, they use filtering software. To ensure the practice of Shabbat, the holiest day of the Jewish week, they turn off their web sites during the time of Shabbat.

2.1.2 System

In this thesis, we use Thomborson's definition of a system as an entity that interacts with another entity (Thomborson, 2010). This definition includes system security framework, hereafter called Thomborson's System Security Framework (TSF). In the TSF, the minimal system is a single sentient constitutional actor which owns to itself. Thomborson (2010) states "the constitution of a system contains a listing of its actors and their relationships, a specification of the interactional behaviour of these actors with other internal actors and with other systems, and a specification of how the system's constitution will change as a

result of its interactions". In TSF, a system which has at least one sentient actor is a sentient system, and a system without a sentient actor is called an automaton. Sentient systems mentioned in the Quran are "angels", "genie", "human beings", and "animals". These systems are subsystems of the universal system. There could be other sentient systems, but we are unaware of these subsystems of the universal system. Since our focus in this thesis is on a societal system, we consider only those sentient systems that relate to a society. Thus, these systems are "human beings" and "animals".

In a society, there are also some systems which are not sentient, and these systems are owned by humans. According to the Quran, the human is the viceroy of *Allah* on earth, and everything on earth is made for humans and everything is subjugated to humans. Therefore, the sentient system of animals is owned by humans, so the minimal system in a society would be a single constitutional human being. In any Quranic-based society, the constitution of a human being is Quranic *Ahkam*. Computer systems are subsystems of the societal system. These systems are also owned and controlled by humans.

According to the Quran, *Allah* is the ultimate owner of everything. In a societal system, all non-human beings are made for human use, so the human system is an immediate owner of all non-human being systems. Every human is owned by himself or herself and by *Allah*. Every human owns their free-will, but a person's *Taqdeer* is owned and controlled by *Allah*. Human actors are sentient actors while non-human are automatons. At a minimum in a society, there would be a single constitutional human actor. According to Thomborson (2010) actors can also have multiple aliases. An alias of an actor is the role which he plays (Thomborson, 2010). We say that an actor has at least two aliases: *Taqdeer* and free-will. The alias *Taqdeer* is more powerful than all other aliases of a human being. Through this alias, all other aliases of a human can be controlled if *Allah* wants (Inshah-Allah).

In a Shariah-based system, a judge as an expert in the *Shariah* defines and verifies the constitution of a system. In defining a constitution for a software system, a judge can seek assistance from a software system expert. Alternatively, a software system specialist can propose a draft constitution, and a judge can alter it to define actual constitution. In a Shariah-based system, the constitution of a system is always harmonious with the Quranic *Ahkam*. The constitution of a Quranic-harmonised software system is essentially a set of

requirements specified for the software system in accordance with the Quranic *Ahkam*.

2.1.3 Stakeholders

Users of a system are often considered the only stakeholders in the system. However, other people can be stakeholders as well. In the RUP, a stakeholder is defined as "an individual who is materially affected by the outcome of the process (*i. e.*. the deliverables the process produces)" (Rational Software Corporation, 2005). In some other studies, a system stakeholder is considered an individual who is either affected by the system or who affects the system (Potts et al., 1994; Kotonya and Sommerville, 1998; Pouloudi and Whitley, 1997). Leffingwell and Widrig (2000) indicate that those who affect a system, for example regulatory bodies, essentially are also affected by the system . Nunes Leal Franqueira (2009) includes attackers of a system as its stakeholders. According to Nunes Leal Franqueira (2009), attackers influence a system by compromising its confidentiality, integrity and availability, *i. e.*. its security. We note that attackers are stakeholders of a system even if they do not compromise system security because system designers and developers, in designing a secure system, pay special consideration to prevent or mitigate attacks. In other words, attackers affect a computerised system even if they do not compromise system security.

2.1.4 System requirements

In this thesis, by "requirement" we mean a Quranic *Hukm*. In the *Shariah*, *Hukm* is defined as a communication from the Lawgiver (*Allah*) concerning the conduct of the *Mukallaf*, and it consists of a demand, an option, or an enactment (Kamali, 1993). Kamali, an eminent contemporary scholar of the *Shariah*, explains that a demand is usually communicated either as a command or a prohibition.

According to Kamali (1993), when a demand is communicated in emphatic terms, it is called *Waajib* (obligation). When a demand is not utterly emphatic, it is called *Mandub* (recommended). An utterly decisive prohibition is called *Haraam* (forbidden). If a prohibition is not utterly decisive, it is called *Makruh* (deprecated). An option allows for individual's choice, and this type of *Hukm* is known as *Mubah* (neutral). Quranic *Ahkam* are of five types, so every requirement would be one of the five types. The five types of

Ahkam are explained in detail in Chapter 3.

Like the Quranic notion of requirement, the RUP has its own definition of requirement. In the RUP, a requirement is "a condition or capability to which the system [being built] must conform" (Oberg et al., 1998). The Institute of Electrical and Electronics Engineers (IEEE) defines a requirement as "a condition or capability needed by a user to solve a problem or achieve an objective" (IEEE, 1990). Alexander (2010) himself writes "Industry still believes that requirements are standalone imperative statements". The grades of exigency in the Quranic *Ahkam* show how requirements do not necessarily have to be imperatives. Thus, the Quranic notion of requirement is more comprehensive and detailed when compared to the notion of requirement in the RUP and IEEE. Quranic *Ahkam* not only specify conditions, they also specify the origin of these *Ahkam* and mention people who are responsible for the accomplishment of *Hukm* or requirement. All Quranic requirements fall on humans.

In the case of software systems, requirements of humans are delegated to software systems. Jackson (1997) also shares his opinion in saying that requirements are located in the real world "the environment" which is distinguished from a software system to be built. Similarly, Jin (2006) considers a system as some part of a reality, and the system is separated from its environment by a boundary and can be observed to interact with its environment. Jin (2006) argues that in requirements elicitation for a system, its environment has an important role. According to Jin (2006), software systems are built to bring about some desirable effects in the environment. Jin (2006) further mentions that requirements are normally not directly concerned with the software system but with the environment with which the software system will interact and in which its effects will be observed and evaluated.

2.1.4.1 Requirements of Muslim stakeholders

Requirements of Muslim system stakeholders are statements which detail their fears and desires associated with a system. The relationship between an individual and *Allah* affect these requirements. According to the *Shariah*, the relationship between an individual and *Allah* is complete submission of the individual to the will of *Allah*. Submission to the will of *Allah* means following all commandments of *Allah*. These commandments

or *Ahkam* are present in the Quran and in the *Sunnah* of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*).

According to the Islamic notion of complete submission to the will of *Allah*, every Muslim must follow the *Ahkam* of *Allah* in each and every sphere of his or her life. Therefore, all requirements of Muslim system stakeholders must comply with the principles of the Quranic *Ahkam*.

To fulfil the requirements of Muslims, especially in financial systems, different Islamic states harmonise these system with the Quran. To indicate how and why the requirements of Muslim stakeholders are addressed in a banking system, Maali et al. (2006) analyse the Islamic banking system for Islamic social reporting. Islamic social reporting is an important aspect of addressing the requirements of Muslim stakeholders of a financial system.

While acknowledging the provision of *Huqooq-ul-Ibad* by the *Shariah*, Maali et al. (2006) mention that the *Shariah* imposes strong social obligations on individuals and organisations. For a banking system, Maali et al. (2006) derive an obligation and an associated right from the *Shariah*. Maali et al. (2006) assert that *Ummah* have a right to know how a bank that is part of the *Ummah* affects the well-being of *Ummah*. Although Maali et al. (2006) did not say so directly but apparently they assumed *Ummah* is an important stakeholder of a banking system. This implies that operations of a Quranic-compliant system which affect its stakeholders must be transparent to the stakeholders, and system owners are obliged to keep their systems transparent to its stakeholders. In Quranic-compliant financial systems, *e. g.*, a Quranic-compliant banking system, system owners discharge this obligation by exercising social reporting (Maali et al., 2006; Vinnicombe, 2010). A *Shariah* advisory committee which often consists of Islamic jurists decides what information a financial system owner, in exercising social reporting, should disclose to system stakeholders (Maali et al., 2006).

Zainul et al. (2004) report some concerns of Muslim stakeholders of an e-commerce system. To harmonise the business practices of an e-commerce system with the Quranic principles, Zainul et al. (2004) specify some general Quranic requirements. These requirements specify the rights and obligation of producers and consumers who are stakeholders in an e-commerce system.

Zainul et al. (2004) state privacy as a right of consumers and emphasise on safeguarding the right to privacy. Zainul et al. (2004) are right in acknowledging the importance of the right to privacy in an e-commerce system, but Zainul et al. (2004) seem on more dubious ground when they argue for safeguarding the privacy of system stakeholders. Zainul et al. (2004) are probably wrong when they argued that consumers or stakeholders would not have any privacy protection in an e-commerce system. We think Zainul et al. (2004) are mistaken because they overlook an important notion of privacy requirements engineering in an e-commerce system. We believe privacy of consumers in an e-commerce system could be safeguarded by engineering and fulfilling Quranic privacy requirements with due diligence.

Despite significant work done on Islamic banking and finance, we think an appropriate response to the Quranic concerns of Muslim stakeholders in software systems has remained relatively unexplored. We do not find any software development process or methodology which provide guidance for addressing the concerns of Muslim stakeholders in software systems. Analyses of Maali et al. (2006) and Zainul et al. (2004) mainly concerned about the Quranic notion of the business practices in electronic financial systems. It appears that Maali et al. (2006) and Zainul et al. (2004) did not pay much attention to underlying software technology to harmonise it with the Quran. We believe this thesis is an appropriate beginning to address the concerns of Muslim stakeholders in software systems.

2.1.4.2 Sources of requirements

In the RUP, the sources of requirements are classified into two types: human (sentient) and non-human (automaton) sources. Human sources of requirements for a system are system stakeholders. System stakeholders include partners, users, customers, domain experts, and system analysts. The three main non-human sources of requirements of a system are existing descriptions of the organisation in which the system is to be used, and information about a similar system, and regulatory constraints. Regulatory constraints are often contained in legal texts.

In the case of a Quranic-compliant software system, system stakeholders, including Muslim system stakeholders, if any, are the human sources of requirements. The Quranic *Ahkam* are a non-human source of requirements for this Quranic-compliant system.

2.1.4.3 Types of requirements

System requirements are often classified as functional and non-functional. Functional requirements are things that a system must do, whereas non-functional requirements are qualities the system must have (Pfleeger and Pfleeger, 2009). Security, privacy, accuracy, and safety are all examples of non-functional requirements (Cysneiros and do Prado Leite, 2004). Pfleeger and Pfleeger (2009) complain that non-functional aspects of systems receive less attention than functional aspects. They further mention that within the category of non-functional requirements, the privacy RE process is less mature than that of security engineering; underlying engineering principles can give little attention to privacy requirements. Pfleeger and Pfleeger (2009) also conceded with an example that privacy requirements can be in conflict with security requirements.

2.1.5 Requirements elicitation

Solving the right problem is of paramount importance in system development (Rumbaugh, 1994). In a system the right problem can be stated by correctly eliciting user's needs of the system. For eliciting user's requirements, Rumbaugh (1994) advocates using use-cases.

The term "elicitation" is relatively new in the RE literature and is often referred to as collection, capture, acquisition, gathering, identification, invention, development, discovery, and fact-finding (Coulin, 2007). For the development of information systems, Davis (1982) used the term "determination" in the same context of elicitation. In giving an overview of RE, Nuseibeh and Easterbrook (2000) preferred the term elicitation. In the software engineering community, the term elicitation is used to indicate that good requirements cannot just be collected from the customer, as it is indicated by the name requirements gathering (Longjun et al., 2010). In this thesis, we use the term elicitation. However, other terms like collection, capture, acquisition, gathering, identification, determination, invention, development, discovery, and fact-finding are considered synonymous with elicitation.

Requirements elicitation is considered to be the first stage in building an understanding of the problem that the software is required to solve (Longjun et al., 2010). Notwithstanding the importance of requirements elicitation, there is very little uniformity in RE

research and practice concerning a standard definition for requirements elicitation (Zowghi and Coulin, 2005). Zowghi and Coulin (2005) describe requirements elicitation a complex process involving many activities with a variety of available techniques, approaches, and tools for performing them. Hickey and Davis (2004) define requirements elicitation an activity of learning, uncovering, extracting, surfacing, or discovering needs of customers, users, and other potential stakeholders . Requirements definition, requirements gathering, requirements elicitation, and RE all aim at figuring out what to build (Holtzblatt and Beyer, 1995). In the RUP, requirements elicitation is defined as "the set of activities that teams employ to elicit or discover stakeholder requirements" (Oberg et al., 1998).

Among other stakeholders, regulatory bodies whose requirements are often contained in legal texts are important stakeholders (Nambisan, 2002). Legal texts are increasingly playing critical roles in requirements elicitation: particularly systems in which non-compliance can entail penalties on their owners (Otto and Antón, 2007). In US, Health Insurance Portability and Accountability Act (HIPAA) requires data holders to protect people's medical information held with them. In US, work is being done to identify HIPAA legal requirements for systems having privacy implications (Breaux and Antón, 2008). For people's privacy protection, the developments made towards forming privacy protection laws are varied in nature and are sometimes even conflicting (Cannataci, 2009).

Cannataci (2009) argues that to have a better understanding of an individual's privacy, we need to investigate the origin of deeper privacy values, their development, and their future directions. In his analysis on privacy, he earmarks religions and cultural values as two essential sources of privacy. His analysis mainly circulates around five massive religions in the world—namely Islam, Christianity, Hinduism, Chinese traditional religions, and Buddhism. However, he does not exclude other religions and cultures and states that they also contain some notion of privacy.

Cannataci (2009) mentions that although every major religion has something to say about an individual's privacy, none of them regulates privacy concerns in present day technological systems.

> These massive religions which for so often and for so long have presented themselves as having all-encompassing ethics systems capable of dealing with

> so many facets of daily life, from the food one eats to sexual activity during or after menstrual cycles, have been remarkably silent on the rights and the wrongs of Internet filtering or CCTV [closed-circuit television] surveillance or biometric passports (Cannataci, 2009).

We hope that our use of the QuRUP on an identity management system will answer Cannataci's negative observation. By using the QuRUP, we will indicate how the Quranic sense of right and wrong could be specified for technological systems. We express right and wrong as requirements in the PIdM in the form of five types of *Ahkam*. For the PIdM, we will elicit these requirements from the Quran. Below we discuss the process of requirements elicitation in the RUP. In Chapter 4, we will customise the RUP for the purpose of eliciting requirements from the Quran.

2.2 Requirements elicitation in the RUP

The RUP is represented by five primary elements. These five elements are "role", "activity", "artefact", "workflow", and "discipline". In the RUP, requirements elicitation activities are contained in the requirements discipline. In the RUP, a discipline is a container which contains a collection of tasks or activities that are related to a major area of concern within the overall project (Rational Software Corporation, 2005). The requirements discipline is one of the core disciplines of the RUP. Other core disciplines of the RUP are business modelling, analysis and design, implementation, test, and deployment.

In the terminology of the RUP, a workflow is a sequence of activities that produces a result of observable value. In UML, a workflow can be expressed as a sequence diagram, a collaboration diagram, or an activity diagram. In the RUP, a workflow is not considered a restricted concept that system engineers must follow exactly and mechanically.

A role defines a set of related skills, competencies, and responsibilities of an individual or group of individuals working together as a team (Rational Software Corporation, 2005). An activity is a unit of work that an individual in a role performs. Activities produce meaningful results.

An artefact is a piece of information produced, modified, or used by a process. Stakeholder requests is an artefact in the RUP. In the RUP, this artefact contains any type of

requests or requirements that a stakeholder might have on the system. It may also contain references to any type of external sources to which the system must comply. This artefact is an output of the activity elicit stakeholder requests; however, it is an input for developing use-cases and developing supplementary specification. Supplementary specification is a requirements artefact in the RUP.

Requirements are likely to be met if an organisation properly manages them. Lack of requirements management decreases the chances of achieving organisational objectives (Oberg et al., 1998). Oberg et al (Oberg et al., 1998) reported that "the Standish Group's CHAOS Reports from 1994 and 1997 established that the most significant contributors to project failure relate to requirements". Incorrect, inaccurate, or imprecise requirements are highly likely to result in unsatisfactory software system, schedule delays, wasted of money, or dissatisfaction of system stakeholders. Requirements elicitation is therefore on of the most crucial parts in the development of software systems.

In the RUP, activities related to requirements elicitation are contained in a discipline called "requirements". The requirements discipline is one of the nine main disciplines of the RUP. In the terminology of the RUP, a discipline is a container which contains related activities. In the requirements discipline of the RUP, it is explained how to elicit stakeholder requests and transform them into software requirements. The system analyst is responsible for the performance of elicit stakeholder requests. In the RUP, elicit stakeholder requests is carried out in the following four steps. These four steps are determine sources for requirements, gather information, conduct requirements workshops, and evaluate your results. Below is a brief overview of these steps.

1. Determine sources for requirements

   In this step, system analysts identify and prioritise human and non-human sources of requirements. System stakeholders are human sources of requirements. Human stakeholders include system users, partners, domain experts, developers, and administrators. Descriptions and design documents of related existing systems, required changes in existing computerised system, and descriptions of organisation for the intended system are examples of non-human sources of requirements.

An important non-human source for requirements are any descriptions of the organisation which will use the system. If a related software system already exists, then this existing system may be read and analysed to determine requirements for a new system. If the new system is an improvement in an existing software system, system analysts should then look for what are change requests. These change requests serve as an important source of requirements for new system.

In the case of a new system which is an automation of an existing manual system, descriptions of the manual system can serve as a source of requirements of new systems. System-related technical expertises of RE team members are also a potential source for identifying requirements for the system.

2. Gather information

   In this step, the RE team formulates questions for the stakeholders of the system. Interviews, questionnaires, and storyboards are recommended techniques in the RUP to gather information from system stakeholders.

3. Conduct requirements workshops

   In this step, the RE team meets with system stakeholders to gather comprehensive requests of stakeholders. Stakeholders' feedback in workshops determine the priority of requirement. Brainstorming and idea reduction, role playing, and use-cases are three examples of techniques in requirements workshops.

4. Evaluate your results

   In this step, elicited requests are evaluated. In results evaluation, it is ensured that there is a priority given to each request and the source of each request is mentioned. Obvious inconsistencies between the requests are also clarified in this step. In the RUP, it is paramount that a select set of customer or users review the results of the requirements workshop in a review or follow-up session . In this session, RE team can identify if there are any issues still needing clarification.

2.3 Requirements elicitation techniques

The RE community has proposed many techniques to capture requirements. Alexander (2010) writes that there is no one way to do RE; rather, there are many ways to accomplish this important phase of system development . The availability and adoption of various requirements elicitation techniques in software development adds weight to the Alexander's statement.

In this thesis, we provides a brief introduction to some requirements elicitation techniques. Readers interested in knowing more about requirements elicitation techniques should consult Leffingwell and Widrig (2000) or Coulin (2007). Below is a summary of some well known and widely used requirements elicitation techniques.

2.3.1 Interviewing and questionnaires

Interviewing with a selected group of key stakeholders is one of the most useful techniques for gathering information. This technique is considered the most traditional and common technique for requirements elicitation (Holtzblatt and Beyer, 1995). Interviews provide an efficient way to collect large amounts of data quickly. The results of interviews, such as the usefulness of the information elicited from stakeholders, vary significantly depending on the interviewer's skill (Goguen and Linde, 1993). The process of interviewing usually consists of four main steps: the identification of stakeholders for the interview, the preparation of the interview, the interview itself and the documentation of the interview's results (Escalona and Koch, 2004).

After conducting several rounds of interviews, the same information appears over and over again. Such recurrence in the interview process allows for creating a set of questions with typical answers. From these answers, stakeholders choose answers that they think are appropriate. The questionnaire technique is no substitute for interviews. It can, however, be very effective when applied after the initial interviewing and analysis activities (Leffingwell and Widrig, 2000).

2.3.2 Requirements workshops

The requirements workshop provides a framework for applying the other elicitation techniques, such as the brainstorming and idea reduction, storyboarding, role playing, and

reviewing existing requirements. These techniques can be used on their own or they can also be combined. The purpose behind the requirements workshop is to make the RE team meet the stakeholders of the system and elicit a comprehensive "wish list" from the system stakeholders.

Focus groups, a well documented social science research method, is a variation of requirements workshop, and focus group has also been used in analysing requirements of software systems (Hall et al., 2002). A system analyst is often the facilitator of the requirements workshop. However, Leffingwell and Widrig (2000) recommend an outsider, experienced in conducting requirements workshops, to facilitate the requirements workshop . Below are common techniques in the requirements workshop.

1. Brainstorming and idea reduction

   Brainstorming is a short group session where every stakeholder present in the session is allowed to say whatever they feel is important to the project. The information gathered through brainstorming is typically informal. Requirements engineers further process this informal information to eliminate any outrageous ideas. Leffingwell and Widrig (2000) describe the following phases for the process of information gathering through brainstorming.

   > Brainstorming has two phases: idea generation and idea reduction. The primary goal during idea generation is to delineate as many ideas as possible; the goal is breadth of ideas, not necessarily depth. The preliminary goal during idea reduction is to analyse all of the ideas generated. Idea reduction includes pruning, organising, ranking, expanding, grouping, refining, and the like (Leffingwell and Widrig, 2000).

2. Storyboarding

   Storyboarding is a technique for capturing logical and conceptual descriptions of system functionality for a specific scenario. In storyboarding, facilitators illustrate the system behaviour to system stakeholders (often users). The stakeholders then comment on this illustration so storyboards evolve in "real time" during the workshop. This technique is commonly used in requirements elicitation for systems involving

user system interactions (Antón and Potts, 1998).

3. Role playing

   Members of the requirements elicitation team are assigned roles of interest to the system. Examples of roles are end users, other systems with which the system under discussion interacts, and subsystems of the system. This technique allows the RE team members to experience the user's world by playing their roles. The technique of role playing is particularly useful when key system stakeholders are missing, so members of requirements elicitation team can take the role of these system stakeholders (Hickey and Davis, 2003). Similar to the technique of role playing "scripted walkthroughs" and "class responsibility collaboration (CRC) cards" are also information collection techniques (Leffingwell and Widrig, 2000). These three techniques are often combined with each other.

4. Review existing requirements

   Examining the documentation of existing and related systems and applications is useful for gathering early requirements for new systems. Often this documentation is coupled with system requirements specifications and requirements specifications from previous or otherwise related systems for reference. These requirements can be reviewed to discover requirements for new systems.

2.3.3 Use-case modeling

Jacobson (2004) first used the term "use-case" in 1986. After that software engineers further developed the concept of use-cases, and now use-case modeling is one of the favoured techniques in industry for eliciting requirements (Lee et al., 1998). In use-case modeling, requirements engineers elicit and specify requirements from the user's point of view (Nasr et al., 2002). Jacobson (1992) describes a use-case as "related sequences of interactions between a user and a system to do something useful". In this description, we note that the system is distinguished from its actors (users). Both the system and its actors perform a use-case. However, in the following definition of use-cases given by Booch et al. (2005), a use-case is accomplished by the performance of an action or actions by a system.

> A use-case is a description of a set of sequences of actions, including variants, that a system performs to yield an observable result of value to an actor (Booch et al., 2005).

Some readers may get confused in understanding who performs in a use-case. We resolved this ambiguity in the definition of use-cases by considering a rather general definition of system. A piece of software is a system, and a user or actor is also a system. When we say a system performed an action, it could mean that a human actor performed an action, or it could also mean that a software system did something.

Use-cases identified in requirements elicitation process also apply to other processes in software life cycle because use-cases are applicable not only in requirements elicitation but also in specifying system requirements. They are also used in system testing (Nebut et al., 2006).

In use-case modeling, the UML use-case diagram is an example of a graphical representation of the use-cases of a system, and each use-case description describes one aspect of the functionality of the proposed system. A use-case description consists of various textual description fields. the use-case name, use-case summary or description, preconditions, and postconditions are four examples of textual description fields of a use-case description. There could be other texual description fields in the description of a use-case.

Some readers might think that the Quranic *Ahkam* may be defined as a textual description field in a use-case description. For example, the Quranic *Ahkam*, which are essentially constraints, may be defined as preconditions or postconditions in a use-case description. Alternatively, Quranic *Ahkam* may be a textual description field, other than preconditions or postconditions, in use-case descriptions.

We argue that it would be inappropriate to consider the Quranic *Ahkam* as preconditions, postconditions, or any other textual description field of the use case descriptions. We first consider preconditions or postconditions. These constraints in use-case descriptions are independent statements (sometimes separate use-cases) that must be true either before or after the execution of a use-case. By contrast, *Ahkam* constrain the use-case (or a certain action or inaction) itself. In other words, the *Hukm* of a statement is not meant to constrain an act prior or posterior to its commission or non-commission. Moreover, *Ahkam*

sometimes have important preconditions and postconditions. The preconditions and postconditions of *Ahkam* and use-cases describe the sequence of certain system actions, states, or use-cases.

It is also inappropriate to represent the Quranic *Ahkam* by adding them as a textual description field, other than preconditions or postconditions, to use-case descriptions. The reason for this is if system engineers represent the *Ahkam* by adding textual description fields to use-case descriptions then this information becomes less accessible and understandable to system users. The Akhamic classifications of use cases are of primary importance to Muslims, who must obey Allah's commands to do, or to refrain from doing, certain acts under certain circumstances (preconditions). Muslims also want to receive guidance from Allah on what is better or worse to do, even when these actions are not absolutely required or forbidden. Therefore, to properly manage the *Ahkam*, we need to alter the use-case diagram and use-case descriptions. We extend the use-case diagram to the Ahkamic diagram, by adding a single word (the Akhamic classification) to the use case. We discuss the Ahkamic diagram in Section 2.4.

The UML use-case diagram is built with the UML elements actor and use-case. The diagram depicts use-cases, actors, and associations among them. Actors are often used to model the users of the system, and they represent the world outside the entity (Dano et al., 1997). A human being or another system can be actors of use-case diagram (Bittner and Spence, 2002). Use-cases are used in a use-case diagram to visualize the functionalities that the system provides to the system users. In a use-case diagram, an actor can take part in several use-cases, and a use-case can interact with several actors (Escalona and Koch, 2004).

In the RUP, use-case modelling technique is used for requirements elicitation. The RUP is a use-case-driven software engineering process. In a RUP-based analysis, a system analyst uses the use-case modelling technique for requirements elicitation. In the RUP, use-cases can also be used as group work for requirements elicitation. In the RUP, it is recommended that the group in a use-case workshop contain people with different backgrounds, knowledge and experience.

Particular sequences of action in a use-case are called scenarios. The terms scenario

and use-case have often been used synonymously (Lee et al., 1998; Rubin and Goldberg, 1992; Glinz et al., 2001; Lund et al., 1996; Allenby and Kelly, 2001). Despite the popularity of use-cases in requirements elicitation, they are, nonetheless, less helpful in the elicitation of non-functional requirements of systems. However, a variation of use-cases called misuse cases are used in conjunction with use-cases to elicit and model some types of non-functional requirements. Below we discuss misuse cases in their use in requirements elicitation.

2.3.3.1 Misuse case modeling

A number of papers have focused on eliciting security requirements by extending use-cases. For example, Sindre and Opdahl (2000) followed independently by McDermott and Fox (1999) describe misuse and abuse cases respectively. The work described by Sindre and Opdahl (2000) is further elaborated upon by Alexander (2002, 2003) to extend the use-case paradigm to specify unwanted behaviour. In a misuse-case-based approach, additional use-cases are used to mitigate or prevent attacks. These additional use-cases are also called security use-cases (Firesmith, 2003). Use-cases are interactions of users with the system, but attack mitigation or prevention for every kind of attack cannot be done in general through additional interactions or security use-cases (Firesmith, 2003).

In order to specify functionality that is not wanted in a system, Sindre and Opdahl (2000, 2005) suggest misuse cases as an extension of use-cases. Misuse cases are essentially use-cases from an attacker's point of view. Use-cases are considered a good tool for specifying functional requirements of a system, but they are less helpful in specifying security requirements. Misuse cases were introduced to overcome the security issue of use-cases and to deal with an unwanted behaviour which is actually an action or set of actions initiated by a misuser. A misuse case is defined as a sequence of interactions between a misuser and a system which leads to harm of a system or of a stakeholder of the system (Sindre and Opdahl, 2005; McDermott and Fox, 1999).

To indicate modelling of use-cases and misuse cases in UML, we show a simple use-cases model of the PIdM in Figure 2.1. In this figure, we model two actors, namely data subject and data holder. We assume that App-CNIC is a use-case and False-App is a misuse case. Data subject and data holder interact with the use-case App-CNIC. In this use-case,

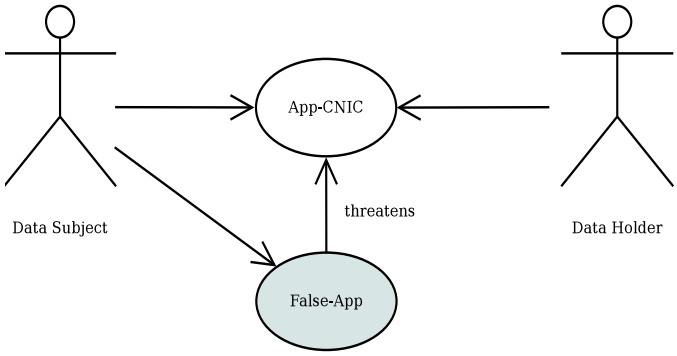

Figure 2.1: *Use-case model for PIdM*

data subject lodges an application for obtaining a CNIC. Through this use-case, data holder obtains the application of the data subject. Figure 2.1 indicates that the data subject may play the role of an attacker. In doing so, the data subject provides false information in his/her application for obtaining a CNIC. We model this behaviour of the data subject as a misuse case, and this misuse case threatens a use-case which is a legitimate way of lodging an application.

Despite some weaknesses, use and misuse cases are widely used in modelling security requirements for a system (Sindre and Opdahl, 2005; Pauli and Dianxiang, 2006; McDermott and Fox, 1999; Fernandez et al., 2006); however, Jorgensen (2001) argued that use-cases cannot specify obligatory actions.

> The use-case states what the user does, and what the machine does in response, but the use-case cannot declare that the user "shall [should]" do anything (Jorgensen, 2001).

Requirements engineers can generate security requirements from a misuse case analysis; however, these requirements are specifications of what the system should not do, that is, system actions that are forbidden. We do not know of any analysis, comparable to use-case or misuse-case analysis, which can generate requirements on what a person is forbidden to do when interacting with a system, or on what a person is obligated to do (*i. e.* forbidden not to do). Recently, access control systems have been extended to cover privacy and digital-rights management systems, but this extension requires explicit consideration of

obligations (Park and Sandhu, 2004). We believe that these analytic difficulties could be resolved by specifying requirements in accordance with the Quranic *Ahkam*. The Quranic *Ahkam* specify what action a human should and should not do, is liked and disliked, and is optional to do.

Another major problem with a misuse-case-based technique is that it may miss some important threats (Fernandez et al., 2006). To overcome this major problem, scenarios-based approaches are proposed (Fernandez et al., 2006; Braz et al., 2008). Below we discuss scenarios and their usage in requirements elicitation.

2.3.3.2 Scenarios construction

Scenarios have also been used in requirements elicitation (Holbrook, 1990; Sutcliffe et al., 1998; Ralyté et al., 1999; Haumer et al., 1999; Cysneiros and do Prado Leite, 2004; Maiden and Robertson, 2005). The software engineering community recognise scenarios as an effective means for eliciting, validating, and documenting software requirements (van Lamsweerde and Willemet, 1998; Gregoriades and Sutcliffe, 2005). Park et al. (2009) used scenarios in eliciting user's requirements in a Robot-based Construction Automation (RCA) project.

Sutcliffe et al. (1998) define a scenario as "one sequence of events that is one possible pathway through a use-case". They generate scenarios for a use-case by walking through each event sequence in the use-case, by applying heuristics which suggest possible exceptions and errors at each step. This analysis is helpful for analysts to specify two pathways. One pathway is for normal behaviour and the other pathway for abnormal behaviour in a system. Each pathway is a scenario. Many scenarios may be specified for one use-case and each scenario represents an instance or example of potential events. A related collection of the scenarios which specify abnormal behaviour may constitute a misuse case.

A use-case is a collection of scenarios. Each use-case provides one or more scenarios that indicate what a system performs in interacting with its end users or with another system to achieve an observable result. Like use-cases, scenarios do not typically consider the internal structure of the system and require an incremental and interactive approach to their development. Sikora et al. (2010) used scenarios at different levels of abstraction. Sikora et al. (2010) called the users and system interactions "system scenarios". They named

the interactions between components of a system as "component scenarios". Component scenarios are the sequence of activities that a computer system performs to accomplish or achieve a specific task.

We define a scenario as "a non-empty set of system actions or system inactions whose performance or non-performance respectively causes benefit or harm to a system stakeholder". We say that if a scenario whose accomplishment or non-accomplishment causes benefit to a system, then it is a positive scenario; if its accomplishment or non-accomplishment causes harm to a system, then this scenario is a negative scenario. van Lamsweerde and Willemet (1998) also used positive and negative scenarios in requirements elicitation. Negative scenarios model the abnormal behaviour in a system, and positive scenarios model the normal behaviour of a system. Misuse cases are a collection of negative scenarios (Alexander, 2003).

Analysing system actions or activities for security requirements is a requirements elicitation approach which is closely related to scenario-based requirements elicitation technique (Braz et al., 2008; Fernandez et al., 2006). The misuse-activities approach consists of a systematic way to identify system threats to determine security policies instead of introducing a new use-case to stop and/or mitigate these threats. This approach is carried out by the performance of two activities. The first activity is an analysis of interactions in system use-cases. In this activity, every interaction is analysed to uncover related threats if any. The second activity of this approach entails a selection of appropriate security policies which can stop and/or mitigate the threat elicited in the previous activity. The combination of security policies and their implementation can be used to harmonise the behaviour of system's user with organisational policies (Parkin et al., 2009).

Braz et al. (2008) is an improved form of Fernandez et al. (2006). In Braz et al. (2008), authors consider the type of misuse and the role of attacker. They ascribe confidentiality, integrity, availability, and accountability (CIAA) as four main types of misuse in a system. They called these types of misuse as "security attributes" and further classified these security attributes into fifteen sub security attributes. These subsecurity attributes are traffic analysis, covert channels, inference, and information disclosure, unauthorised data modification, transactional integrity, deception, masquerading, spoofing, impersonation, denial

of service, disruption, repudiation, and track erasing. By using Braz et al. (2008) for security requirements elicitation, they claimed to uncover more threats by considering the type of misuse, and threats from insiders. The type of misuses in Braz et al. (2008), is quite similar to threats elicited by Solove (2006) in his privacy taxonomy. The misuse-action approach might be more promising than the misuse-case base approach because the misuse-action approach may uncover more threats. However, like the misuse-cases approach the misuse-action approach also focuses on prohibited actions. These techniques lack support for eliciting other types of requirements like obligation. With the similarities between requirements elicitation and *Ahkam*, extending the UML use-case diagram into an Ahkamic diagram lends itself to modelling Quranic requirements in an existing UML artefact. We develop an example of five possible types of scenarios modelled in the Ahkamic diagram in the next Section.

2.4 The Ahkamic diagram

An Ahkamic diagram is a diagram that shows a set of system scenarios or *Far* and actors and their relationships. This diagram is useful for eliciting and communicating Ahkamic requirements to system stakeholders. We believe that communicating any system requirement in Ahkamic form is an appropriate way to make requirements understandable to Muslim system stakeholders.

Rumbaugh (1994) insists for structuring system requirements, but he also does not ignore the importance of understandability of requirements to system stakeholders. Rumbaugh (1994) emphasises that "the requirements must be expressed in some structured way, but they still be understandable to the users who must verify them." We think that system requirements modelled in the Ahkamic diagram would be understandable to Muslim system stakeholders. The details of the Ahkamic diagram might be explained in the description of the Ahkamic diagram. In this thesis, we do not argue that our diagrams are the only, or the best, possible description of an Ahkamic requirement. However we do encourage requirements engineers to use our Ahkamic diagrams when communicating with Muslims, unless they are confident they have found a better method.

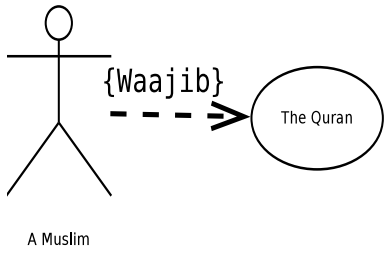

Figure 2.2: *The minimal Ahkamic diagram*

The Ahkamic diagram is an artefact which is an extension of the UML use-case diagram. Far, actors, and relationships among them are artefacts of the Ahkamic diagram. We model these three artefacts of the Ahkamic diagram by three constructs of UML: use-case, actor, and relationship arrow. In the Ahkamic diagram, we model Far by the use-case construct, and actors are modelled by using the actor construct of UML. Arrows in Ahkamic diagram depict relationships. We label the arrows between actors and use-case constructs by the type of the scenario (Far). We label the arrows between two use-case constructs as relations extends, include, threatens, and mitigates. The type of a Far is one of the five *Ahkam*. In the Ahkamic diagram, actors (humans) are responsible for performance or non-performance of connected Far. If an actor is another non-human system then the owner of this non-human system is responsible for the performance or non-performance of that specific Far. We do not expect any responsibility from any non-sentient system. Instead, we consider the owners of non-sentient systems responsible for the performance or non-performance of any Far by their owned systems.

Minimally, in the Ahkamic diagram there would be one actor (a human), one Far (the constitution of the human), and one relationship between the actor and Far. For depicting the minimal Islamic system in the Ahkamic diagram, there would be an actor (a Muslim) and a Far (the Quranic *Ahkam*), and the relationship between the actor and its constitution. In this case the relationship would be *Waajib* because it is *Waajib* for Muslims to follow the Quranic *Ahkam*. In Figure 2.2, we model the minimal Ahkamic diagram for an Islamic system.

The Ahkamic diagram expresses Ahkamic requirements. To use this diagram for requirements elicitation, RE teams need three constructs: Far, actors, and relationships. Relationships in Ahkamic diagram are of two types. The first type of relationship is among Far, and the second type of relationship is between Far and actors. Extend, include, threatens, and mitigate are relationship types among Far of the Ahkamic diagram. The system analyst is responsible for specifying these relationships. *Waajib*, *Haraam*, *Mandub*, *Makruh*, and *Mubah* are five possible types of relationships between actors and Far. We call these relationships Ahkamic relationships. The Quranic analyst is responsible for specifying Ahkamic relationships.

We give an example to indicate how an Ahkamic diagram might be used in requirements elicitation and communication. In Figure 2.3, we model an Ahkamic diagram of the PIdM. This diagram is indicative, and the artefacts produced for this diagram are based on our assumption that a system analyst might generate and model the same artefacts. This diagram is an extension of the use-case diagram modelled in Figure 2.1. We assume that the system analyst of the PIdM identifies two actors: data subject and data holder. App, Receive-app, False-info, and Verify-info are scenarios or Far that the system analyst might identify. Verify-info is a Far which mitigates the scenario False-info. App Far specifies a case that a data subject lodges an application. Receive-app is a Far of receiving the application by a data holder of the PIdM. False-Info is a Far in which the data subject provides false information in lodging the application. Verify-info specifies that the data holder verifies the information for correctness.

After the system analyst has identified Far and actors, and relationship between Far, these artefacts are provided to a Quranic analyst. The Quranic analyst who is also a member of requirements elicitation team examines each Far and specified a Quranic *Hukm* for the Far. We assume that the Quranic analyst declares the Far of lodging and receiving an application (App and Receive-app scenarios) as *Mubah*. We also assume that the Quranic analyst might specify the *Ahkam Haraam* and *Waajib* for False-info and Verify-info respectively. As a result of the analyses of the system analyst and the Quranic analyst, we come up with an Ahkamic diagram as depicted in Figure 2.3.

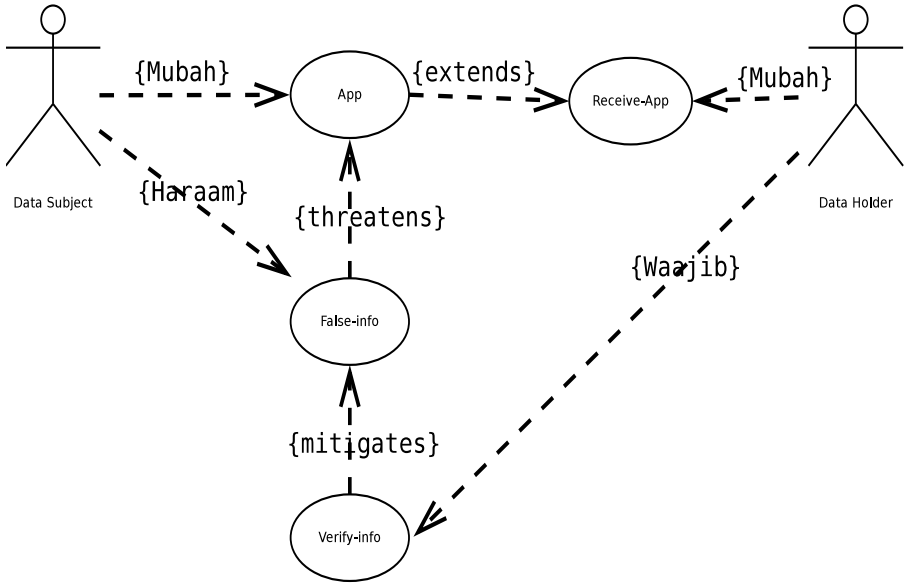

Figure 2.3: *An Ahkamic diagram of the PIdM*

In this chapter, we presented the three types of artefacts (actor and scenarios and relationships) of the Ahkamic diagram, but prior work is needed to arrive at the stage of modelling these artefacts. There are complete processes involved in identifying and modelling these artefacts. These processes will be discussed in detail in subsequent chapters.

Beside being an appropriate means, as indicated in the previous example, to elicit requirements, Ahkamic diagrams are also, arguably, appropriate visual representations to communicate system requirements to Muslim stakeholders. Each Far of the Ahkamic diagram would represent one requirement. Muslims are normally familiar with *Ahkam*. Therefore, we think an Ahkamic diagram is an appropriate choice to communicate system requirements to Muslim system stakeholders. Requirements are communicated to system stakeholders for verification and validation.

Despite of the appropriateness of Ahkamic diagrams in requirements elicitation and validation, these diagrams would be less helpful for directly communicating requirements to software developers for developing a software system. Ahkamic diagrams would be less helpful for system developers because these diagrams depict system wide requirements. In

the RUP or in any other software development process, software developers might be interested in software requirements only and not requirements on people. To communicate requirements to software developers, the use-case diagram is a more appropriate tool. So the Ahkamic diagram would need to be transformed into a use-case diagram to model software requirements and communicate these requirements to software developers. In transforming an Ahkamic diagram to a use-case diagram, the scenarios which place requirements on human's actions and inactions would be eliminated, and these scenarios could be specified in another artefact or diagram. In the RUP, system-wide requirements are contained in the supplementary specification artefact.

2.5 Summary

A system is an entity that interacts with another entity. Every system is a subsystem of another system and every system is an owned system. Allah is the ultimate owner of all systems. The constitution of a system contains information about the system including requirements of the system. In software systems, requirements for these systems are desires and fears of its stakeholders. In software systems, use-case modelling is one of the commonly used techniques for managing requirements of their stakeholders. In use-case modelling, UML use-case diagram are used. The RUP, a well-respected and widely used process for software development, is a use-case driven process. In the RUP, its practitioners employ UML use-case diagram in managing requirements of system stakeholders.

Muslims can be an important stakeholders of a software system. For an appropriate response to the concerns of Muslim system stakeholders, UML use-case diagram is insufficient for managing the requirements of Muslim system stakeholders. For an appropriate management of the requirements of Muslim system stakeholders, we extend the UML use-case diagram to an Ahkamic diagram. We indicate by an example how an Ahkamic diagram might be used in managing requirements of Muslim system stakeholders. In an Ahkamic diagram, the relationship between an actor and a use-case construct is one of five types of *Ahkam*.

CHAPTER 3

Quranic Ahkam on Privacy

Seeking knowledge is obligatory upon every Muslim (Prophet Muhammad)

The most superior among you (Muslims) are those who learn Quran and teach it to others (Prophet Muhammad)

In order to respond appropriately to the Quranic concerns of Muslim system stakeholders, system engineers must know the requirements of Muslim system stakeholders. In this thesis, system requirements are the requirements of Muslim stakeholders associated with a particular system. This thesis uses the term "requirements" which would also mean "system requirements". Our customisation of the RUP which is the QuRUP is a proposed process for eliciting requirements of Muslims system stakeholders. The focus of this thesis in using the QuRUP is on privacy requirements of Muslim stakeholders concerning software systems. This thesis exemplifies the use of the QuRUP by demonstrating an application of the QuRUP on a computerised software system, the PIdM.

The Quran is the main source of guidance for Muslims; they seek Quranic guidance in every part of their lives. In the Quran, there is ample guidance, manifested in the Quranic *Ahkam*, about the protection of people's privacy. We define DoCoMo as the collection

of domestic privacy-related *Ahkam*, people's communication-related *Ahkam*, and people's modesty-related *Ahkam*. The DoCoMo is the private sphere created and safeguarded by DoCoMo *Ahkam*.

DoCoMo *Ahkam* can be used as a potential input to the QuRUP in the process of eliciting privacy requirements for software systems. Chapter 4 indicates the use of DoCoMo *Ahkam* in the QuRUP. In Chapter 5 of this thesis, DoCoMo *Ahkam* are used as an input to the QuRUP for the purpose of eliciting privacy requirements in the PIdM.

The rest of this chapter is organised as follows: in Section 1, Quranic *Ahkam* and their five types are introduced. In Section 2, domestic privacy-related *Ahkam* are reviewed. Section 3 contains Quranic *Ahkam* which safeguard people's privacy by regulating communication with each other. Section 4 deals with the review of Quranic modesty regulations from the perspective of privacy protection. In Section 5, an Islamic reasoning method called *Qiyas* and its potential use for extending DoCoMo *Ahkam* for software system is discussed. Section 6 concludes this chapter.

3.1 Quranic Ahkam

To regulate and secure a society, Allah has specified requirements in the Quran. In every Shariah-compliant system, Allah is the sole owner and creator of all the universe which can be called a universal system. In a society, every system is a subsystem of the universal system. These subsystems are owned by human beings. To design, operate, and govern the subsystems, Allah has provided general requirements for the human beings in the Quran. These requirements are called the Quranic *Ahkam* and these *Ahkam* are documented in the Quran. The Quranic *Ahkam* are of five types: *Haraam*, *Waajib*, *Mandub*, *Makruh*, and *Mubah*. Below we discuss each of these five types.

3.1.1 Haraam (forbidden actions)

In the *Shariah*, *Haraam* denote all those things which are forbidden or prohibited. The performance of an *Haraam* action is punished and their non-performance is rewarded (Shehaby, 1982; Kamali, 2003). Below we give examples of *Haraam* actions.

1. In the following verse of the Quran, few *Haraam* things are described. In this verse an Arabic word Hurraymut has been used for prohibition. The word Hurraymut is a

derivative of the word *Haraam*.

> You are forbidden [Hurraymut] carrion and blood, the flesh of swine and of that animal which has been slaughtered in any other name than that of Allah... (Quran 5:3).

2. In the following verse of the Quran, *Haraam* actions are declared by the Arabic word La.

> Do not [la] usurp one another's property by unjust means nor offer it to the judges so that you may devour knowingly and unjustly a portion of the goods of others (Quran 2:188).

3. The following verse of the Quran declares actions as *Haraam* by associating those actions with Satan.

> O Believers, wine, gambling, (ungodly) shrines and divining devices are all abominable works of Satan: therefore refrain from these so that you may attain to true success (Quran 5:90).

4. In the following verse of the Quran, taking property of orphans by force has been declared as *Haraam* by specifying punishment with this action.

> In fact, those who grab unjustly the property of the orphans, fill their bellies with fire, and most surely they shall be thrown into the burning fire of Hell (Quran 4:10).

3.1.2 Waajib (obligatory actions)

Waajib Ahkam specify obligations which must be done-neglecting them without any genuine excuse is a sin (Khan, 1997). The Islamic principle of Enjoining Good and Forbidding Evil falls under the category of *Waajib*. This principle does not allow one to investigate the private sphere of other's life. Likewise, this principle does not allow one to commit sin in the public domain. Therefore, *Waajib* is a Quranic *Hukm* to deal with the public sphere of human life (Kadivar, 2003). If *Waajib* are the obligations to act, then they may also be called as forbidden inactions because their non-commissioning is also liable to be punished.

3.1.3 Mandub (recommended actions)

Mandub specify all those things which are desirable to Allah but not required. Doing a *Mandub* action is considered to be a good deed, but not doing these is not considered a sin. Examples of *Mandub* are giving alms (other than the obligatory one) to poor people, attending a sick person, and writing a contract while doing financial transactions (Khan, 1997). In the *Shariah*, a *Mandub* action is expressed in various forms as explained below.

1. An order followed by an indication that this order is a recommendation. This kind of expression for a *Mandub* is present in following verses of the Quran.

   > O Believers, when you contract a debt for a fixed term, you should put it in writing...Quran 2:282-283).

   This Quranic commandment says that you should set down in writing the giving and taking of loan. In this verse an Arabic word Fuktuboohu has been used which means to write. The Arabic word for "write" strongly connotes an obligation. But in the rest of the verse it has been stated that if the creditor and the debtor trust each other, then there is no harm if they do not write. This relaxation reduces a *Waajib* to a *Mandub* (Kamali, 2003).

3.1.4 Makruh (deprecated action)

Makruh is opposite of *Mandub* in that it is preferred to omit them than to commit them. Committing them is de-meritorious and not committing them is meritorious (Badr, 1978). Committing is not liable to punishment, but according to Hanafi (an Islamic school of thought), committing a *Makruh* entails moral blame. In the *Shariah* a *Makruh* action, is expressed in various forms as explained below.

1. Explicit use of word *Makruh* or its derivative. In the following verse of the Quran, various actions of a human being are declared as *Makruh* by using Arabic word *Makruh*.

   > The evil aspect of each of these Commandments is odious [*Makruh*] in the sight of your Lord (Quran 17:38).

2. A prohibition followed by an indication that this prohibition is a *Makruh*.

> O Believers, do not ask questions concerning such things, which, if made known to you, would only vex you; but, if you will ask such questions at the time when the Quran is being sent down, they will be made known to you. Allah has forgiven what you have done so far: for He is Forgiving and Forbearing (Quran 5:101).

3.1.5 Mubah (permitted actions)

The *Mubah* is an Arabic term which denotes an action as neither forbidden nor required or recommended, and so religiously neutral. The merely permitted actions, *i. e.*. those one may or may not do (*Mubah*), are relatively greater in number than all other actions. In other words ample room for human beings to decide according to their needs and deeds within the limits of the *Shariah* is provided. A good intention of a doer turns a *Mubah* into a *Mandub* and a bad intention turns a *Mubah* into *Makruh*. Some examples of *Mubah* in the *Shariah* are given.

1. Offer of betrothal to a woman
   The action of an offer of betrothal to a woman is declared as *Mubah* as is clear from the following verse of the Quran.

   > It is no offence if you make indirect proposal of marriage to widows during their waiting term or keep it concealed in your hearts: for Allah knows that you will naturally think of them. But be careful not to make any secret engagement. If you have to do anything, do it in an honourable way. And you should not settle anything finally about the marriage until the waiting term expires. Understand it well that Allah even knows what is hidden in your hearts; so fear Him. Also know that Allah is Lenient and Forgiving (Quran 2:235).

2. All Halal things, an act of eating food belonging to people of the Book, and marrying a chaste woman who is follower of a Book of Allah are both *Mubah*. The following verse of the Quran reveals these *Mubah*.

> All the good and pure things have today been made lawful for you; the food of the people of the Book is lawful for you, and your food for them, Likewise you are permitted to marry chaste believing women or chaste women from among the people who were given the Scripture before you provided that you give them their dowries and become their protectors in wedlock; this permission is not for sensual license or secret illicit relations; whoever rejects the way of Faith, all the deeds of his life shall become vain and he shall be a bankrupt in the Hereafter (Quran 5:5).

3. All things in their original and natural states are also *Mubah*
   In the *Shariah*, there is a rule that all things are *Mubah* if there is no ruling specified about them. This freedom is a gift from Allah to humankind, as indicated in the following verse of the Quran.

   > He it is Who created for you all that there is on the Earth; He then turned to the sky and ordered it into seven heavens. And He has full knowledge of everything (Quran 2:29).

The aforementioned five types of Quranic *Ahkam* regulate a societal system by specifying requirements concerning the actions and inactions of humans. However, some systems like computer systems are not regulated explicitly in the Quran. To seek Quranic *Ahkam* for such systems, a judge (an expert of the Quran) interprets, often relying on *Qiyas*, a related general Quranic *Ahkam*. In software systems, we must ensure Muslim stakeholders' actions satisfy these five types of *Ahkam*. In order to perform an Ahkamic analysis in software systems, an Islamic jurist who is expert in the *Shariah* must interpret the Quran to specify an extension of the Quranic *Ahkam* for software systems. In this thesis, we indicate how these *Ahkam* might be extended to specify privacy requirements for software systems.

For different purposes, Islamic scholars have been analysing the Quranic *Ahkam* for centuries. In this thesis, we provide a brief summary of their analyses on the primary *Ahkam* relating to people's privacy. Below some Quranic *Ahkam* which constitute and safeguard the DoCoMo are reviewed.

3.2 Houses-related Ahkam

The Quran protects people's domestic privacy by restricting entries to their houses and by restricting loitering near other people's houses. It not only prohibits entering other people's houses, but it also restricts entry of family members in their own houses. The Quranic *Ahkam* define the family house as a private place: an area that is secure against unwelcome intrusions by outsiders and insiders.

3.2.1 Entering another person's house

The Quran contains several sets of verses that define rules for restricting access to residential spaces. The following verse of the Quran defines the protocol for entering someone else's house.

> O Believers, do not enter other houses than your own until you have the approval of the inmates and have wished them peace [Salaam]; this is the best way for you: it is expected that you will observe it (Quran 24:27).

In the above verse, an Arabic word (La tadkhuloo) is used in the phrase translated as "do not enter". This connotes a *Haraam*, or absolute prohibition. In the explanation of the above Quranic verse, Maududi translates the Arabic word "tastanisu" used in the above verse as approval. He mentions that the word tastanisu is derived from the Arabic root word "uns" which means fondness, affection, or regard. Therefore, a visitor should seek approval of inhabitants and not just their permission. In other words, the visitor must make sure that his entry in the house is not disagreeable to the inmates and he is sure of a welcome. That is why Maududi translates the word "tastanisu" as "approval" of the inmates instead of "permission" of the inmates, because the word "approval" expresses the sense of the original more precisely. The Arabic equivalent to permission is the word "tastazinu". Seeking only permission does not fully fulfil the purpose of the word "tastanisu". One can conclude that this verse demands a visitor to seek a joyous permission before entering someone else's house. In this verse, the other condition on a visitor before entering some one else's house is to offer *Salaam* to the inhabitants of the house.

Quranic protection of protection is not only from an individual or group of individuals but the Quran also safeguards one's domestic private sphere from any intrusions from a

government. On the basis of the following story of an Islamic ruler, Hayat (2007) concludes that Islam respects individual's freedom and his right to privacy, and it does not allow any Islamic state to invade in people's privacy.

> Hadrat Umar Bin Khattab, the second caliph, was roaming in the city one night when he heard shouting and cursing coming from a residence; he then peeked over the perimeter and started admonishing the man: 'You, the sinner, do you think that God will ignore your sins, as you're sinning against him?' The man replied: 'Woe, commander of the faithful, do not rush to judgement; if I sinned once, you sinned three times. God has forbidden you to look into someone's fault, and you have done otherwise. God has commanded you to enter peoples' homes through the front door, and you have intruded over the fence. And you have approached me without salutation, and God has commanded you not to enter into other peoples' homes without their permission, and without saying 'greetings' (Salaam) when you enter their premises'. Hadrat Umar reportedly asked for the man's forgiveness, and went on his way only after he was granted it (Hayat, 2007).

This story is also mentioned in Maududi's explanation of the Quran. Maududi states that the indubitable Islamic principle of *Amr-bil-Maroof*-wa-*Nahi-anil-Munkar* also does not allow an Islamic government to invade people's privacy. Kadivar, an Iranian Islamic philosopher is of same opinion to Maududi, and he mentions that the Islamic principle of enjoining good and forbidding evil applies only to the public sphere of one's life. A *Muhtasib* is usually designated by Islamic states to do surveillance of public places and ensure compliance of Islamic principles at these places. The *Muhtasib* is not allowed to investigate or invade people's privacy, even if they are committing sin in their privacy (Kadivar, 2003).

3.2.1.1 Entities within a house

The Quran not only protects people's privacy from being watched or listened in their houses, it also protects their privacy by safeguarding entities within their houses. On the basis of his analysis on the work of Muslim jurists, Alshech (2004) argues that one of

the reasons that domiciles receive immunity is due to the sensitive nature of their contents. Alshech (2004) reports that al-Zamakhshari indicates that certain locales are protected because people deposit in them things that they wish to keep secret or private. Al-Zamakhshari whose full name is Abu al-Qasim Mahmud ibn Umar al-Zamakhshari is one of renowned scholar of Mutazilite school of Islam.

The Quranic immunity to entities in people's houses, because houses protect people from public scrutiny is clear from following verse of the Quran.

> Then, if you do not find anyone therein, do not enter until you have been given permission, and if you are told to go back, you should go back. This is a purer way for you; and Allah has full knowledge of what you do (Quran 24:28).

Without permission any entry into other people houses is *Haraam* even if no one is present inside the house. If inhabitants of a house refuse a visitor from entering to their house, then it is *Waajib* for the visitor to go back. The above verse indicates that it's not only the owner whose privacy has been protected but also all entities and activities within a house. Therefore, one can say that privacy of all people and their entities and activities within a house is also protected.

3.2.1.2 Timely arrival and leaving concerning other people's houses

In the following verse of the Quran, believers are commanded to arrive on time for an invited meal, and do not stay any longer after taking the meal. These commands for arriving on time and dispersing soon after eating the meal protect some other value(s) of the house's owner.

> O you who have believed, do not enter the houses of the Prophet without permission, nor stay watching for the meal time; but if you are invited to meals, do come, and when you have taken food, disperse. Do not engage in talk and discussion, for such behaviour causes trouble to the Prophet but he is shy of saying anything, and Allah does not feel shy in telling the truth. If you have to ask the wives of the Prophet for something, ask for it from behind a curtain. This is a better way for the purity of your as well as their hearts (Quran 33:53).

Although in the above verse, Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) is the focal point, according to Maududi, this commandment is applies equally to all people. "Sallallahu Alaihi wa Sallam" is an Arabic expression which Muslims use whenever the name of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) is mentioned or written. The meaning of this Arabic expression is "May the blessings and the peace of Allah be upon him (Muhammad)". According to the Quranic verse 33:53, it is a *Haraam* act to sit in someone's house to eat meal without invitation because one may not be able to serve meal for all uninvited guests, thus causing possible humiliation for him. When on is invited to a meal, it is *Haraam* to sit there past the end of the meal, because sitting longer in other people's houses may disturb their peace of mind or trouble them, and may impede execution of their domestic activities. On the basis of the above verse, while taking an instrumental approach to privacy, one can conclude that people's houses are regulated to protect their peace of mind. Moreover, according to this verse it is *Waajib* for a male to talk to non-mahram women behind a curtain whenever he has to talk. Mahram is an Arabic term which means "unmarriageable kin", so non-mahram denotes a person that one can marry and should therefore obey the rules of modesty.

3.2.2 Entering one's own house

The Quran not only prohibits entering other people's houses without permission, it also demands a proper entry to one's own house. Firstly, it prohibits entering one's own house secretly. In the following verse of the Quran, believers are commanded to enter their house through their front doors only.

> They ask you about the phases of the moan[moon]. Say, "These are signs for the people to reckon dates and fix the periods for hajj." Also tell them, "It is no virtue to enter your houses from their backs during the Hajj days; real virtue is that one should refrain from incurring the displeasure of Allah; so enter your houses by their proper doors, and fear Allah so that you may gain (true) success" (Quran 2:189).

During the life time of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*), Arabs had a bad habit of entering their own houses from the back when they were in condition of *Ihram*.

Likewise, when they returned from an uncompleted journey, they would enter their houses by jumping over the walls or through windows in the back of their houses. They used to consider this action as a virtue. In order to eliminate this bad habit, the above verse was revealed. In this verse we notice two important things. The first one is refraining from displeasure of Allah. The second thing is success which can be gained by fearing Allah and obeying his orders. In the context of above verse, refraining from displeasure of Allah is refraining from entering the houses from any opening except the front. This means that entering houses from the back is a *Haraam* action. The non-righteousness declaration of one's act of entering into his own house is indicative that this act is *Haraam*. Also in the context of the above verse, fearing Allah and gaining success means one must enter houses from their proper doors. Therefore, entering houses through their proper doors is a *Waajib* action.

In the Quranic verse 2:189, apart from diminishing a bad custom, privacy of a house's inhabitants is protected from their own family members: entering a house by jumping over the walls or through windows in the back of the house could jeopardise the privacy of those inside. In such situations, a house's inhabitants would not have enough time to adjust themselves to protect their privacy from the person who enters the house by jumping over the walls or through windows.

The following verse of the Quran defines the protocol for inhabitants of a house who have relatively more access to the house.

> O Believers, your slaves and those of your children, who have not yet become sex conscious, must ask your permission before coming in to see you on three occasions: before the Fajr Prayer and at noon when you put off your clothes and after the 'Isha' Prayer. These are your three times of privacy. There is no sin for you or for them if they come without permission at other times than these, for you have to visit one another over and over again. In this way Allah makes His Commandments clear to you for He is All-Knowing, All-Wise (Quran 24:58).

In the above verse, Allah specifies three times of a day as private times for a house's owner. In this verse, restrictions are imposed on children and slaves. Since Islam has eliminated the concept of slavery. So instead of specifying requirements on children and slaves, one can use a related term servant for slaves.

The above verse indicate that it is *Waajib* for people who have frequent access in a house to seek permission before entering into the house during the owner's private times. However, it is *Mubah* for these people to enter the house at other times. It is *Waajib* for the house's owner to make sure that all people who have frequent access to the house are aware of these rules (Maududi, 1987).

The following verse of the Quran indicates that it is *Waajib* for older children to seek permission before entering their home.

> And when your children have grown sex conscious, they should receive your permission for this just as their elders get permission. In this way Allah makes His Revelations plain to you for He is All-Knowing, All-Wise (Quran 24:59).

So far in this thesis, Quranic *Ahkam* have been reviewed which provide immunity to people's houses. This immunity is either an end in-and-of itself or it is instrumental in protecting some other values like preventing a social catastrophe. But what about public buildings and shops? The following verse of the Quran reveals that entry is not prohibited to such buildings.

> There is, however, no harm if you enter houses which are not dwelling places, but contain something useful for you; Allah knows what you disclose and what you conceal (Quran 24:29).

From this verse, Maududi concludes that it is *Mubah* to enter a building, such as a shop, hotel, or guest house, which is generally open to all people.

3.2.2.1 Protocol for Offering Salaam

The English translation of the Arabic word *Salaam* is peace. In an electronic communication in which data holders get information from data subjects, we consider *Salaam* as an assurance from the *Salaam*-offering party that they are not attackers and they will

not harm data subjects. *Salaam* is the most shortened version of the Islamic greeting "As-salamu Alaikum wa rahmatullahi wa barakatuh", and it originates from the Hebrew greeting "Shalom". A derivative of *Salaam* is "Al-Salaam" which is one of the 99 names of Allah in Islam. In Islamic societies, Al-Salaam is used in conjunction with abd to denote name of an individual. Abd Al-Salaam is a name which translates to "Slave of Al-Salaam" (*i. e.*. Slave of Allah). Because of the holiness of the word *Salaam*, one is not permitted to greet one another with the word *Salaam* in unholy places such as a bathroom. In Judaism, Shalom is also considered a holy word an it is used in similar contexts to its usage in Islamic system. Shalom is used for greeting, as a name of God, and as a name of an individual.

Below some *Ahadith* are quoted from the Quranic explanation of Maududi. These *Ahadith* explains the Quranic verse 24:27.

> A man named Kaladah bin Hanbal went to see the Holy Prophet and got seated without the customary salutation. The Holy Prophet told him to go out and come in again after calling: Assalam-o-alaikum (peace be upon you).
>
> It is related that whenever Hadrat Umar went to see the Holy Prophet, he would say: "Assalam-o- alaikum ya Rasul-Allah, I am Umar: May I enter!".
>
> The Holy Prophet enjoined that permission should be asked thrice at the most. If there is no reply even at the third call, one should come back.
>
> Once he [Prophet Muhammad (*Sallallahu Alaihi wa Sallam*)] went to the house of Hadrat Sad bin Ubadah and sought permission twice after greeting with: Assalam-o-alaikum wa Rahmatullah (peace be upon you and mercy of Allah), but there was no response. After calling for the third time when he received no response, he turned back. Sad came out running from the house, and said, "O Messenger of Allah, I was hearing you all right, but I desired to have Allah's peace and mercy invoked upon me through your sacred tongue as often as possible; therefore, I was replying to you in a low voice" (Maududi, 1987).

Alshech (2004) argues in his analysis on the Islamic notion of domestic privacy that most Muslim scholars adopted an instrumental approach to privacy, in which these Muslim

scholars viewed privacy not as an end unto itself but rather as a means to promote a viable society, to prevent their community from disintegrating, and, ultimately, to enshrine the Islamic principles in a society. Alshech (2004) further mentions that the Islamic protection of privacy is not only to promote well-being of a family or society, it also benefited individuals whose privacy was protected. This is because, according to him, the Islamic protection to any interference with an individual's peace of mind, which is secured by the immunity of domiciles, has no direct affect on his or her family or clan. According to him Muslim jurists in promulgating regulation about privacy protection viewed the well-being of an individual as no less important than the social well-being of the family.

3.3 Communication-related Ahkam

The private sphere delineated by the Quran is not confined to the domestic realm. In addition to to safeguard people's domestic private sphere, Quranic *Ahkam* restrict people's communications. Quranic *Ahkam* which regulate people's communications provide a security wall around an individual. One of the values safeguarded by the creation of a private zone through this security wall is people's honour. In a communication related *Hukm*, the Quran prohibits people from spying and having too many suspicions about others. This prohibition is clear from the following verse of the Quran.

> O you who have believed, avoid much suspicion, for some suspicions are sins. Do not spy, nor should any one backbite the other. Is there any among you who would like to eat the flesh of his dead brother? Nay, you yourselves abhor it. Fear Allah, for Allah is Acceptor of repentance and All-Merciful (Quran 49:12).

Keeping excessive suspicions about others, to be curious about other's private matters, and back-biting are treated equivalent to eating the flesh of one's own dead brother. This clearly indicates that Allah dislikes all these actions. Therefore, these are *Haraam* actions. In the case of keeping excessive suspicions, the intruder can be considered as communicating information about an individual, and this communication of information is an attack on the individual's honour. Also, in harbouring excessive suspicions, the intruder constructs and communicates to himself a set of bad information about other person. As for back-biting,

the intruder communicates some harmful information about the individual to other people. In these two cases, one can imagine that information flows into the security wall by associating this information with an individual. However, in the case of spying, information about an individual flows out of the security wall. With spying, the intruder collects information about an individual that may damage the individual or create profit for the spy.

Maududi emphasises that one must not spy on others. He mentions that whether spying is done because of suspicion; for causing harm, or for satisfying one's own curiosity, it is forbidden by the *Shariah* in every case. It is not appropriate for a believer to try to peep at other people from behind curtains to find out their defects and their weaknesses. According to Maududi, reading other people's private letters, listening secretly to others' conversations, peeping into a neighbour's house, and trying to get information about the domestic life or private affairs of other people are extremely immoral and therefore are prohibited. Maududi treats back-biting of a deceased person equivalent to back-biting of a living person. If one indulges himself in one of the aforementioned actions, then he should immediately repent to Allah.

Maududi insists that the prohibition of spying is applicable not only to individuals but also to an Islamic government. He says an Islamic government is not allowed to search for people's secrets. Maududi mentions that Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) is reported to have said, "If you [governments] start prying into the secret affairs of the people, you will corrupt them, or at least drive them very near corruption". This Hadith indicates that any invasion through the communication security wall could possibly lead to a social disaster by making people corrupt. One can argue that Quranic communication-related *Ahkam* not only benefit an individual, the promulgation of these *Ahkam* also aim to benefit a society at large.

In addition to spying and back-biting, the Quran imposes a ban on scandalisation and defamation of other people in order to protect their privacy and sanctity of life. This is clear from the following verse of the Quran.

> O you who have believed, neither should men mock other men, it may be that these are better than they; nor should women mock other women, it may be that these are better than they. Do not taunt one another among yourselves, nor

> call one another by nicknames. It is an evil thing to be called by a bad name after faith. Those who fail to avoid this are wrongdoers (Quran 49:11).

Mocking or scoffing other people, defaming other people, and insulting other people by calling them with bad names are all prohibited actions. According to Maududi, mocking does not only imply mocking with the words but it also includes mimicking somebody, making pointed references to him, laughing at his actions or his physical appearance, or calling the people's attention to some defect in him so that others may laugh at him. According to Maududi, scoffing other people, defaming other people, and insulting other people by calling with bad names hurt the other person, which causes mischief to spread in society. That is why these action have been forbidden. Although these three types of actions are often done by words but mocking and defamation can also also be done by actions.

In the following verse of the Quran, there is further support on the prohibition on defaming and back-biting of other people.

> Doomed (to ruin) is every such person who slanders others (in their face) and backbites them habitually (Quran 104:1).

3.4 Modesty-related Ahkam

For people's privacy protection, besides the Quranic *Ahkam* relating to people's houses and people's communication, we must consider modesty-related *Ahkam*. Modesty-related *Ahkam* refer to the Quranic commandments concerning the physical appearance of believers, especially that of women, in their home and in public spaces. Alshech (2007) argues that modesty regulations delineate a private sphere whose purpose is to safeguard some other important values. One of the values safeguarded by the promulgation of modesty-related *Ahkam* is people's honour. The following modesty-related Quranic verses instruct both men and women about protection of their private body parts.

> And O Prophet, enjoin the Believing men to restrain their gaze and guard their private parts. This is a more righteous way for them: Allah has knowledge of what they do. O Prophet, enjoin the Believing [wo]men to restrain their gaze

> and guard their private parts and not to display their adornment except that which is displayed of itself, and to draw their veils over their bosoms and not to display their adornment except before their husbands, their fathers, the fathers of their husbands, their sons and the sons of their husbands (from other wives), their brothers, their brothers' sons, their sisters' sons, their female associates and those in their possession and male attendants incapable of sex desire and those boys who have not yet attained knowledge of sex matters concerning women; also forbid them to stamp their feet on the ground lest their hidden ornaments should be displayed. O Believers, turn all together towards Allah: it is expected that you will attain true success (Quran 24:30-31).

One's act of lowering his gaze and guarding his private parts is described as decent by Allah. These verses indicate that it is *Waajib* for believing men to lower their gazes and protect their private parts, and it is *Waajib* for a believing women to keep herself unexposed to those who are not kin. There is another Quranic verse about protection of private parts.

> Most surely the men and the women who have surrendered themselves to Allah; who are believing, obedient, truthful, and patient; who bow down before Allah, practice charity, observe the fasts, guard their private parts and remember Allah much: Allah has prepared for them forgiveness and a vast reward (Quran 33:35).

In this verse a promise of great reward from Allah for, apart from other good practices, protection of private parts, indicates that protecting private parts is *Waajib* for both men and women. In the Quranic verse 33:36, it is mentioned that if someone does not act according to what Allah has said, then he is in error.

Thus, modesty regulations in the Quranic verses 24:30-31 and 33:35 protect people's honour. For protection of honour of a chaste woman, the following verses of the Quran are relevant.

> As for those persons who charge chaste women with false accusations but do not produce four witnesses, flog them with eighty stripes and never accept their

> evidence afterwards, for they themselves are transgressors, except those who repent and reform themselves; Allah is Forgiving and Merciful (Quran 24:4-5).

If someone accuses a chaste woman of a crime of adultery, then he needs to prove it by bringing four witnesses. If he could not prove the accusation, then a punishment of eighty stripes are mentioned in the Quran for him. Moreover, his witness in the future will be never accepted and he is also a transgressor–An English translation of Fasiq, until he repents from Allah. According to the majority of Islamic scholars, repentance vindicates him from transgression, but it does not exonerate him from the prescribed punishment of eighty stripes and deprivation from the right of witness. While explaining the above verse Maududi states that if one repents, then Allah forgives only the punishments of hereafter, but wordily punishments are not forgiven. According to Maududi protection of honour is not limited to a chaste woman but also applies to a chaste man. False accusation of a chase person is a *Haraam* act with the same punishment.

The aforementioned modesty-related *Ahkam* delineate a private sphere for protecting people's honour. (Alshech, 2007) thinks that Muslim jurists have understood some areas of a woman's body, at least in some respects, to have been an extension of the family's private sphere even though they were physically located on a woman's body. He thinks on this line on the basis of the ruling of the *Shariah* in which kin were allowed to see (and sometimes touch, provided the touch was platonic) some of these zones of woman's body. From the work of Muslim jurists on modesty regulations, (Alshech, 2007) tends to conclude that modesty regulations benefit the family as whole and not the individual needs of women. The essence of Alshech's analysis on modesty-related *Ahkam* is that these *Ahkam* create and safeguard a private sphere, and the purpose underneath delineating this sphere is to protect other important values.

Qiyas is a method in the *Shariah* through which Quranic *Ahkam* can be extended for matters not regulated explicitly in the *Shariah*. In this thesis, we use this method to extend Quranic *Ahkam* for software systems. In using *Qiyas*, the main focus of this thesis is on extending relevant DoCoMo *Ahkam* for specifying privacy requirements in software systems. In the next Section, a brief introduction of *Qiyas* is provided, with an indication of its application for deriving Quranic *Ahkam* in software systems.

3.5 Qiyas (analogical reasoning)

The *Shariah* comes from two primary sources of Islamic law. These two primary sources are the Quran and the *Sunnah* of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*). Muslims believe that the Quran contains the words of Allah. These worlds were revealed to Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) through revelation by an angel Jibreel. The Arabic word *Sunnah* means habit or usual practice. In the *Shariah*, the *Sunnah* refers to the practices of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*). The text of the Quran and *Sunnah* of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) are finite, and regulate mostly the known problems of the time of revelation (Mohammad, 2001). After the death of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*), the process of revelation stopped because Muslims believe that Muhammad (*Sallallahu Alaihi wa Sallam*) was the final messenger of Allah. And there is no more messenger to come after him. In order to determine the rule intended by Allah for any matter which is not explicitly regulated in the Quran or *Sunnah*, the principal method adopted by Sunni Muslim jurists is *Qiyas*.

In the *Shariah*, *Qiyas* is considered an extension of a legal ruling from an *Asl* to a *Far*. Only an Islamic jurist (or judge) can perform *Qiyas* reliably. The end-result of a *Qiyas* is a *Hukm* (ruling or judgement). When performing *Qiyas*, the judge looks for the *Illah* underlying the *Asl*. If an identical or similar *Illah* is found in the *Asl*, then the *Hukm* in the *Asl* can be extended to the *Far*. In the *Shariah*, rulings derived via *Qiyas* are not considered to be new laws; instead they are considered as an extension of existing law (Kamali, 2003). The *Illah* behind an *Illah* is called *Hikmah* or rationale (Moghul, 1991).

While some Islamic scholars say the Quran and *Sunnah* are the only primary sources of the *Shariah*, others believe that the primary sources of the *Shariah* are the Quran, *Sunnah*, *Ijma* (consensus of Islamic jurists), and *Qiyas* (Serour, 1993; Schenker, 2002). Kamali states that the primary sources of the *Shariah*, in their order of priority, are the Quran, *Sunnah*, *Ijma* and *Qiyas* (Kamali, 2003). Kamali based his argument on the following verse of the Quran.

> O Believers, obey Allah and obey the Messenger and those entrusted with authority from among you. Then if there arises any dispute about anything, refer it to Allah and the Messenger, if you truly believe in Allah and the Last Day. This is the only right way and will be best in regard to the end (Quran 4:59).

Kamali, in explaining the above verse of the Quran, states that "obeying Allah and the Messenger" means seeking guidance from the Quran and *Sunnah*. He further states that "those from among you who are invested with authority" refers to *Ijma*, and "referral of disputes to Allah and the Messenger" refers to *Qiyas*.

In *Qiyas*, the Quranic ruling of an original case is extended to a new case on the basis of their shared *Illah*. *Illah* can be identified by the Quranic text or it can be established by consensus of Islamic jurists (Kamali, 2003). Islamic jurists have already identified the *Illah* behind most of the Quranic verses. In this article, we base our analogical reasoning process mostly on previously identified *Illah* underneath a Quranic verse.

There are four essential elements of *Qiyas* called its arkan, or pillars. These four pillars of *Qiyas* are *Asl*, original case; *Far*, a new case; *Illah*, effective cause which must be found to be shared by both *Asl* and corresponding *Far*; and hukm al-asl, the ruling of the original case that is extended from the *Asl* to the *Far* if the *Illah* is common to both (Moghul, 1991). We call these four pillars as tasks of *Qiyas*.

Sowa and Majumdar (2003) have provided a simple example of *Qiyas*, which we summarize below. It is written in the Quran that grape wine is prohibited, but nothing is said about date wine. The *Hukm* for date wine would be derived as below.

1. *Asl* (original case): Drinking grape wine is prohibited.
2. *Far* (new case): Is drinking date wine prohibited?
3. *Illah* (effective cause): Drinking grape wine is prohibited because it is intoxicating; drinking date wine is also intoxicating.
4. *Hukm*: Drinking date wine is also prohibited.

Qiyas is applied to seek *Hukm* for matters not explicitly regulated in the Quran or *Sunnah*. A *Hukm* derived by *Qiyas* has varying degrees of reliability, depending on how carefully

Illah was identified and how much *Illah* is obvious underneath *Asl* and underneath *Far*. However, any conclusions drawn by *Qiyas* are at least somewhat speculative because of the involvement of human opinion in reasoning process (Kamali, 2003).

3.6 Summary

The Quran specifies requirements on the actions and inactions of human being. Quranic requirements or *Ahkam* are of five types. In this chapter, we review *Ahkam* related to privacy. We synthesise privacy-related *Ahkam* to DoCoMo. DoCoMo consists of domestic, communication, and modesty related *Ahkam*. It is a comprehensive review of privacy-related *Ahkam*.

We review *Qiyas* which is a process to extend Quranic *Ahkam* for matters not regulated by the Quran. System analysts can use *Ahkam* of DoCoMo as a source in *Qiyas* to specify software requirements harmonised with the Quran. In the QuRUP, we use the tasks of *Qiyas* to extend *Ahkam* of DoCoMo to specify requirements for software systems. We do not extend all *Ahkam* of DoCoMo in specifying software requirements through the QuRUP.

CHAPTER 4

Quranic Rational Unified Process

Whoever guides or directs to good, then he gets the same amount of blessing as the one who does it (Prophet Muhammad)

Quranic requirements elicitation in software systems is an important and essential activity for an appropriate response to the concerns of Muslim stakeholders in these systems. The concerns of Muslim system stakeholders are their fears and desires associated with a system. In order to respond appropriately to the concerns of Muslim stakeholders of software systems, we propose the QuRUP, a duly diligent process. We describe an application of the QuRUP on the PIdM to elicit Quranic privacy requirements for the PIdM. The QuRUP is our customised form of the RUP.

In Chapter 3, we reviewed five types of *Ahkam* promulgated in the Quran by particularly focusing on *Ahkam* constituting and safeguarding the DoCoMo. The DoCoMo is the private sphere constituted and safeguarded by domestic regulations, conversational regulations, and modesty regulations. Domestic regulations are those Quranic *Ahkam* which give sanctity to one's privacy in its house. Conversational regulations are those Quranic *Ahkam* which safeguard people's reputation by ascribing their conversations as private and by putting restrictions on disclosing the contents of other people's talks. Modesty regulations are Quranic *Ahkam* which create and safeguard private zones on the bodies of human

being. Following the review on *Ahkam* safeguarding the DoCoMo, we explain *Qiyas* and its use in extending Quranic *Ahkam* for matters not explicitly regulated in the Quran.

In Chapter 2, our literature review on system stakeholder requirements elicitation, we did not find any technique or process which is earmarked for eliciting Quranic requirements to fulfil the needs of Muslim system stakeholders. To elicit these requirements, we choose and customise the RUP to the QuRUP. In the following section, we discuss a model of the QuRUP. In Section 4.2 of this chapter, we explain how the QuRUP could be used to elicit Quranic requirements of Muslim stakeholders of a software system. In Section 4.3, we give a comparison of the QuRUP with the RUP. Lastly, in Section 4.4, we conclude this chapter by summarising the work of this chapter and indicating an abstract of the work performed in Chapter 5.

4.1 A model of the QuRUP

In Figure 4.1, we present a simplified flowchart for a QuRUP-based software development. The initial activity in a QuRUP-based software development is a preliminary assessment of a project. System analysts review Quranic *Ahkam*, and understand the RUP. After this preliminary work on *Ahkam*, the RUP, and the project, system analysts or any other people who have the power to make decisions about the project decide whether to develop a Quranic software system or not. If the decision is not to develop a Quranic software system, the RUP can be used for system development. In the case of a Quranic software development, system engineers apply the QuRUP for software development. Like the RUP, the QuRUP could be applied iteratively.

Like any other development process, the final output artefact in a QuRUP-based development is a developed system. However, this thesis goes only to the production of system requirements. System engineers then refine system requirements to model use cases. Based on these use cases, developing a software system becomes possible. To produce Quranic-compliant requirements, we customise the requirements discipline of the RUP. The requirements is a core discipline of the RUP. In Figure 4.2, we depict various steps taken towards requirements elicitation.

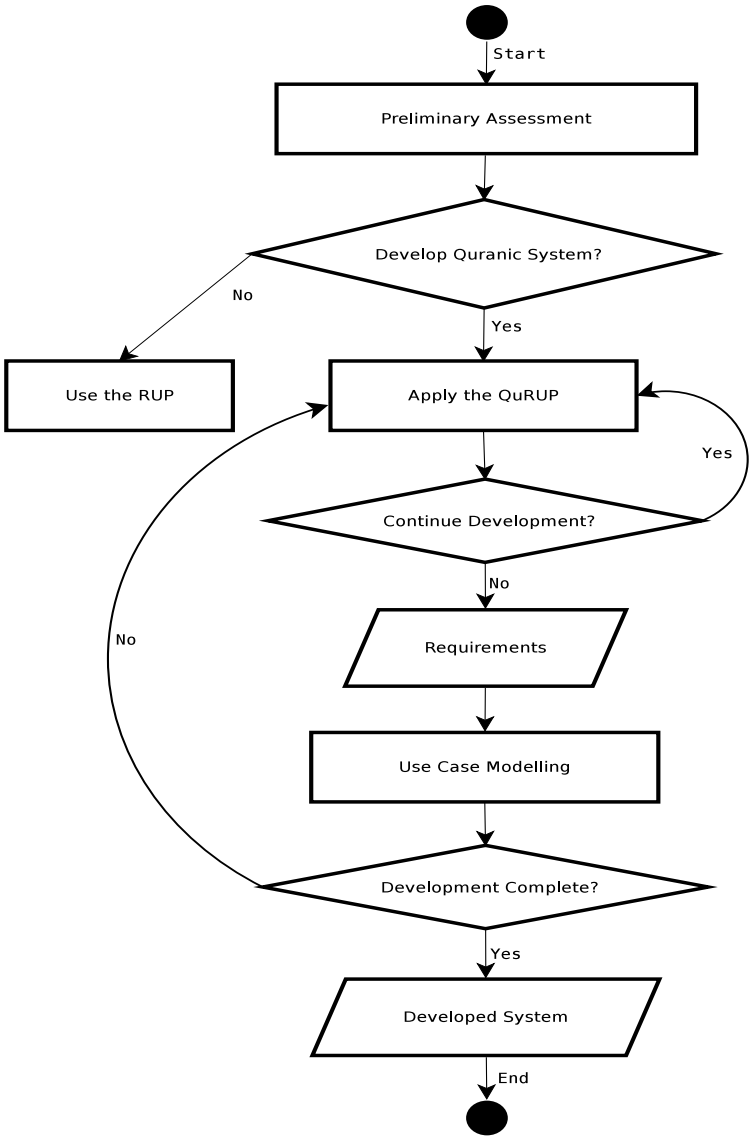

Figure 4.1: *The QuRUP in system development*

Project manager, system analyst, and Quranic analyst are three main roles in the QuRUP. The project manager prepares iteration plans and also manages the overall project. Someone acting as system analyst is expert in technical systems and coordinates in requirements elicitation. Someone acting as a Quranic analyst is one with sound knowledge of the *Shariah*. A Quranic analyst determines Quranic *Ahkam* for software systems.

In an application of the QuRUP, eliciting *Asl* and eliciting *Illah* underneath *Asl* are two activities of a Quranic analyst. *Asl* is a Quranic regulated case, and Illah of a *Asl* is an effective cause underneath *Asl*. Elicitation of *Far* is an activity performed by a system analyst. *Far* is a target case which is not explicitly regulated in the Quran. In the QuRUP, the term "activity" and "task" are used interchangeably. *Far*, Illah underneath *Far*, and Quranic text are input artefacts to the activity elicitation of *Asl*. A statement taken from a Quranic text related to a certain *Far* is an output artefact of the activity elicitation of *Asl*. Project manager decides the time length for the continuation of the QuRUP in system development. When the QuRUP is stopped its output is requirements. Stakeholder requests is an artefact in which our elicited Quranic requirements live. During later stages of software development, the QuRUP can also be reiterated.

Below we explain various activities of the QuRUP. We explain these activities with an example to indicate how the QuRUP can be used for eliciting Quranic requirements of Muslim system stakeholders. In this example, by applying the QuRUP we elicit a privacy requirement for the PIdM.

4.2 The proposed process

Requirements elicitation of Muslim system stakeholders is a sub-problem of the problem of responding to the concern of Muslim system stakeholders. Altering a system that contravenes the *Ahkam* of the Quran would satisfy Muslims who fear to be involved in an unIslamic activity. However, instead of doing alterations in the developed system to meet the requirements of Muslims, it is more appropriate to elicit requirements and then develop the system to meet these requirements. The QuRUP deals with requirements elicitation from the Quran, and the QuRUP produces artefacts for use by system developers in the development of Quranic-compliant systems.

The QuRUP consists of eight steps, and in each step a task is performed by a role. By the performance of these tasks, requirements engineers can elicit religious requirements of Muslim system stakeholders. We depict these steps of the QuRUP in Figure 4.2. Project manager, system analyst, and Quranic analyst are roles which perform the tasks of the QuRUP. In the PIdM, the role of project manager, system analyst, and Quranic analyst are played by *Pero*, *Sam*, and *Qas* respectively.

To exemplify the use of the QuRUP, we elicit one privacy requirement in the PIdM by using the QuRUP. We elicit this requirement of the basis of our experience as CNIC holder of the PIdM. In applying the QuRUP to this example, we play the roles of project manager, system analyst, and Quranic analyst. We assume that people playing these roles will perform their activities identically to how we perform by playing their roles. Below we explain the eight requirements elicitation tasks of the QuRUP.

1. Prepare iteration plan

   Iteration plan is an artefact produced by performing this task. The project manager is responsible for preparing a plan for various tasks in an iteration. Iteration plan consists of a time-sequenced set of tasks or activities, with their assigned resources, for an iteration. The project manager and the members of the RE team use iteration plan. The project manager assigns tasks of an iteration to the members of the RE team. The members of the RE team use an iteration plan to understand what they must do, and when they must do it, and what will be given as an input artefact. In the PIdM, the task of preparing an iteration plan is performed by *Pero*, the project manager of the PIdM. Below we discuss subtasks of the task "prepare iteration plan".

   (a) Make an RE team

   The project manager performs this task. An RE team can be made up from three roles: system analyst, Quranic analyst, and system developer. These roles represent system stakeholders. Although, the members of an RE team are responsible for eliciting requirements, often these people know some system requirements because of being their stakeholder status, or they know some system

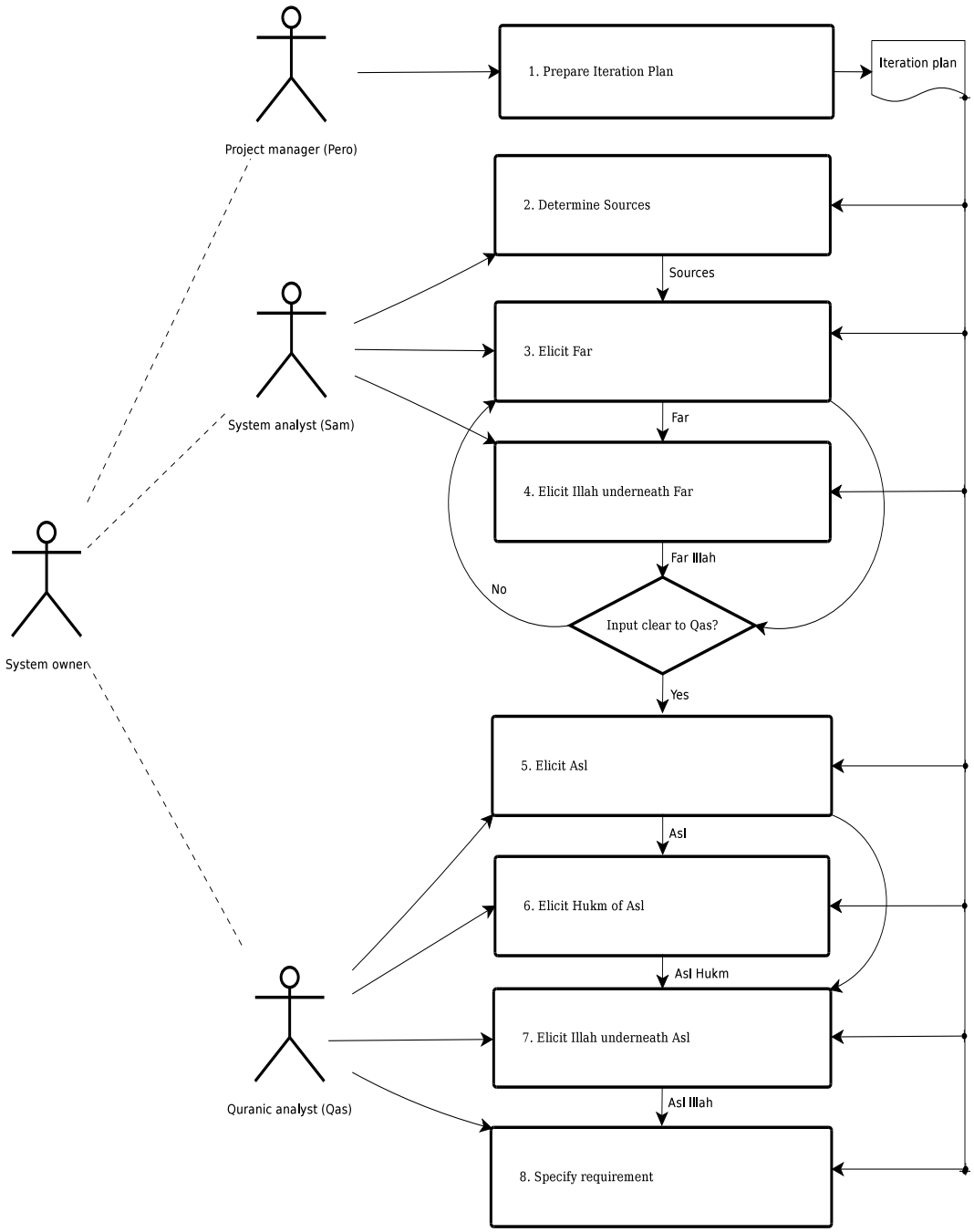

Figure 4.2: *The QuRUP*

requirements because of their knowledge in the area of the system being developed. In the QuRUP we do not restrict the roles to only system analyst, Quranic analyst, and system developer. The project manager of the QuRUP can also include other roles in making an RE team.

(b) Identify tasks of the QuRUP

Again the project manager performs this task. Here, the project manager identifies tasks for requirements elicitation. The project manager also identifies the order in which to carry out these tasks. Additionally the project manager specifies inputs and outputs of each task.

(c) Assign tasks to the RE team

The project manager assigns each role with a particular task. He also specifies the time by which a particular task must be completed.

The output of the task prepare iteration plan is an artefact called "iteration plan". This artefact is an input to the remaining requirements elicitation tasks of the QuRUP.

We assume that *Pero*, the project manager of the PIdM, makes an RE team of two roles: Quranic analyst and system analyst. It is possible for a single person to play both of these roles. In this case, the person needs to be expert in the *Shariah* as well as in technical systems. However, we assume that the project manage assigns the roles of Quranic analyst and system analyst to two different sentient systems. *Sam* and *Qas* are two sentient systems. *Sam* plays the role of system analyst, and *Qas* plays the role of Quranic analyst. We assume that for requirements elicitation in the PIdM, *Pero* might prepare an iteration plan such as that depicted in Table 1. Column 2 of this table presents tasks of the QuRUP, and column 1 is the order in which the tasks in the QuRUP are performed. Elicit *Far* and elicit Illah underneath *Far* are two tasks of the QuRUP which are are assigned to *Sam*. Elicit *Asl*, elicit *Hukm* of *Asl*, elicit *Illah* of *Asl*, and specify requirement are tasks which are assigned to *Qas*. Determine sources is a task assigned to *Sam* and *Qas*. Sys Info (system-related information) and Req (requirements) are input and output artefacts respectively.

2. Determine sources of requirements

Table 1: *An iteration plan for requirements elicitation in the PIdM*

Sequence	Task	Role	Input	Output
1	determine sources	*Qas*, *Sam*	IP, Sys Info.	sources
2	elicit *Far*	*Sam*	IP, sources	*Far*
3	elicit *Illah* of *Far*	*Sam*	IP, *Far*	*Illah*
4	elicit *Asl*	*Qas*	IP, *Far* and *Illah*	*Asl*
5	elicit *Hukm* of *Asl*	*Qas*	IP, *Asl*	*Hukm*
6	elicit *Illah* of *Asl*	*Qas*	IP, *Asl*	*Illah*
7	specify requirement	*Qas*	IP, *Asl*, *Far*, and *Ilal*	Req.

In this task of the QuRUP, the system analyst has primary responsibility for determining human and non-human sources of requirements. The Quranic analyst is an additional performer of this task. In Figure 4.2, we depict only its primary performer. The Quranic analyst is responsible for determining Islamic sources for system requirements. Quranic explanations, collection of *Hadith*, and opinions of jurist(s) are three examples of Islamic sources for system requirements.

System stakeholders are human sources of requirements, but there can also be non-human sources for requirements. System descriptions along with the technical expertise and experience of an RE team members are examples of non-human sources for requirements. It is the job of the system analyst to identify all human and non-human sources of requirements.

For the purpose of Quranic requirements elicitation in the PIdM, we assume that *Sam* uses his experience of interacting with the PIdM as a source of requirements. We also assume that *Sam* uses Solove's categorisation of privacy invasions as another source of requirement elicitation. In the PIdM, *Sam* generates various instances of the invasions identified by Solove (2006). These instances are helpful in requirements elicitation. Our assumption about *Qas* is that he uses the Quranic explanation of Maududi as a non-human source for system requirements.

3. Elicit Far

   The system analyst is responsible for the performance of this task. The Ahkamic diagram has an important role in the accomplishment of this task in the QuRUP. To accomplish this task, the system analyst identifies "actor" and "*Far*" which are two

constructs of the Ahkamic diagram. The relationship between actor and *Far* as the third construct of the Ahkamic diagram is identified and modelled by the Quranic analyst.

A *Far* specifies a possible action of a system stakeholder that he performs while interacting with the system. A *Far* can be elicited by applying an information-gathering technique either alone or in conjunction with another information-gathering technique or techniques. Devising scenarios, conducting interviews, and questionnaires are among well known techniques of information gathering. Through these techniques a *Far* can be constructed. Stakeholder requests, descriptions of a system or related systems, user system interactions, and system related knowledge of the system analyst are inputs to this task. We call these inputs sources of requirements. *Far* is an output artefact of this task.

The system analyst's prior knowledge of the system could be on the basis of his academic background, practical experience, study of a similar system, or through studying scholarly work written on the system or related systems. The system analyst uses his knowledge to construct *Far*. For example, he may rely on the use case method to construct *Far*. The system analyst can obtain knowledge about the use case method from published literature on use case method and its application. He may then categorise each interaction in a use case or misuse case as a *Far*. A system analyst relying on TSF could construct different *Far* on the basis of possible scenarios due to superior-inferior relationships between system stakeholders.

A system analyst relying on Solove's privacy model for requirements elicitation is likely to construct various *Far* corresponding to different types of violation as identified in Solove (2006). Solove (2006) classifies privacy-related harmful activities in four types. These four types of harmful activities are "information collection", "information processing", "information dissemination", and "invasions". Whether it is Solove's privacy taxonomy, the TSF model, or the use case method that the system analyst uses in constructing *Far*, all these are essentially an input to the QuRUP.

We assume that *Sam* uses Solove's classification in modelling *Far* construct of the

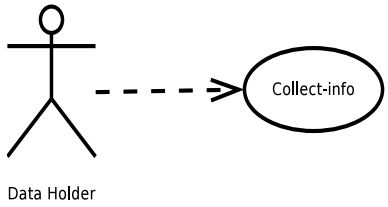

Figure 4.3: *Ahkamic diagram of a data collection scenario*

Ahkamic diagram in the PIdM. Therefore, in the PIdM analysis Solove's classification is an input. We also assume that *Sam* has experience of interacting with the PIdM, and he uses this experience in eliciting *Far*. We indicate how *Sam* might elicit a *Far* in an information collection activity of the PIdM. Based on our experience as CNIC holder, we know that at the time of lodging an application (an information-collection activity for a CNIC), the data holder of the PIdM obtains personal information of data subjects. Based on our assumption that *Sam* would be aware of this action which is an information collection activity of the data holder, he might construct the following *Far*.

Far Collect-Info. A data holder X collects personal information of a data subject Y

Collect-Info and its actor (data holder) are modelled in Figure 4.3. In Figure 4.3, no relationship type between actor and *Far* is mentioned. This relationship will be elicited and modelled in later steps of the QuRUP.

4. Elicit Illah underneath Far

   The system analyst is responsible for the accomplishment of this task. A *Far* elicited in the previous step of the QuRUP is an input artefact to this task of the QuRUP. An *Illah* is an output artefact of this task. The system analyst can elicit *Illah* underneath a *Far* by envisioning a possible consequence after the accomplishment of the *Far*, or through the process of accomplishment of *Far*. Elicitation of *Far* and elicitation of *Illah* under *Far* are two tasks that must be performed before the start of any analysis by the Quranic analyst because the output artefacts of system analyst's tasks are input

artefacts for the Quranic analyst's tasks.

We know that some types of personal information are of sensitive nature. Any disclosure of such information can damage reputations. For example, disclosing information of a certain disease of an individual can damage the individual's public reputation. Disclosure of sensitive information can also cause anxiety and mental distress to the person relevant to the information. However, there are some other types of personal information whose disclosure does not directly cause damage to the person relevant to the information. For example, disclosing an individual's identifying information such as their name, age, and residential address does not apparently seem to damage the person relevant to the information. However, we note that people's identification information is often grouped to create digital dossiers about individuals. These digital dossiers can then be used to harm individuals to whom these digital dossiers correspond. Harm caused by identity fraud is an example of such harm.

Although the act of disclosing identification information in itself may not be a harmful act, future harm from this can occur. In other words, disclosure of someone's identification information could facilitate an attacker in causing harm to the person relevant to the information. Intruders can use a digital dossier to obtain some private information about the individual. We can therefore conclude that collecting personal information of data subjects might be a harmful act, and this act is essentially an entrance into the private sphere of data subjects.

Solove in his privacy taxonomy is explicit in declaring the collection of people's personal information as an entrance into their private domain. Any system analyst who uses Solove's privacy taxonomy as a source for his knowledge is highly likely to conclude the collection of people's personal information is an invasion to people's privacy. In analysing the PIdM, *Sam* uses Solove's taxonomy of privacy as a source of his knowledge. We therefore assume that *Sam* might also consider invasion to the private sphere as a consequence of collecting people's personal information. Below we list this assumption about *Sam* as an *Illah* underneath *Far* 1.

Illah Underneath Far 1. An entrance in private sphere

Far and *Illah* underneath *Far* are input artefacts for eliciting the relationship construct of the Ahkamic diagram. The relationship construct of the Ahkamic diagram is determined by the Quranic analyst. Before reaching the stage of determining the relationship construct of the Ahkamic diagram, there are other necessary intermediate tasks. The QuRUP describes a systemic way of performing these required tasks. These tasks are performed by the Quranic analyst and are explained below.

5. Elicit Asl

   The Quranic analyst is responsible for accomplishing this task. A *Far* and an *Illah* underneath the *Far* are input artefacts to this task. Based on the input, the Quranic analyst finds an *Asl* which is relevant to the input *Far*. *Asl* is an output artefact of this task. If the Quranic analyst has any confusion in understanding the input artefacts which are prepared by the system analyst, then the Quranic analyst should consult with the system analyst to clarify the input artefacts. Both analysts should have an agreement on what is *Far* and *Illah* underneath *Far*. In Figure 4.1, we depict only one check point which is "inputs clear to *Qas*?" to indicate whether or not the inputs are clear to the Quranic analyst. However, the confusion in understanding *Far* or *Illah* underneath *Far* could arise during the accomplishment of any tasks in the QuRUP. At any stage, if confusion arises in understanding inputs, then the Quranic analyst can consult with the system analyst to clarify the requirements.

   In the analysis of the PIdM, the text of the Quran is also an input artefact to this task of the QuRUP. *Qas* uses this text in eliciting an *Asl* which is relevant to the input *Far*. In the application of the QuRUP on the PIdM, *Qas* uses the Quranic explanation of Maududi for eliciting *Asl* which is relevant to the *Far* identified above. We assume that *Qas* might elicit the following *Asl* which is relevant to *Far* 1.

   Asl 1. A person X enters in the house of a person Y

   The above *Asl* is derived from the following domestic privacy protection verse of the Quran.

   > O Believers, do not enter other houses than your own until you have the approval of the inmates and have wished them peace [Salaam]; this is the

best way for you: it is expected that you will observe it (Quran 24:27).

From this verse of the Quran, a *Hukm* will be elicited in the following task of the QuRUP. This *Hukm* will be used later in defining requirements.

6. Elicit Hukm in Asl

   The Quranic analyst is responsible for the accomplishment of this task. A *Hukm* for an *Asl* is often mentioned explicitly in the Quranic text. In some cases, it is not mentioned explicitly. In these cases the Quranic analyst, based on his knowledge of the Quran and his knowledge of the Arabic language, can deduce the *Hukm* for an *Asl*.

   The *Hukm* for *Asl* 1 is clearly mentioned in the Quranic verse 24:27. For *Asl* 1, we assume that *Qas* might also elicit the following *Hukm* conveyed by the Quranic verse 24:27.

   Hukm of Asl 1. No person X is allowed to enter in the house of a person Y

7. Elicit Illah underneath Asl

   The Quranic analyst is responsible for achieving the task of elicit *Illah* underneath *Asl*. An *Asl* is an input artefact to this task. An *Illah* underneath an *Asl* is often mentioned in the Quranic text, and the Quranic analyst can use that *Illah* in a QuRUP analysis. If *Illah* underneath a Quranic verse is not specified, then the Quranic analyst uses his knowledge of the *Shariah* to elicit an *Illah* underneath any *Asl*. Maududi mentions "protection of private sphere" is an *Illah* underneath *Asl* 1. Any Quranic analyst who follows the Quranic explanation of Maududi would specify "protection of private sphere" as an *Illah* underneath *Asl* 1. In *Asl* 1 as identified for the PIdM, we assume that *Qas* might also specify the following *Illah* for the *Hukm* of *Asl* 1.

   Illah underneath Asl 1. Protection of private sphere

8. Specify requirement

   Again the Quranic analyst performs the task of "specify requirement". A requirement is essentially a *Far* along with its Quranic *Hukm*. The output of this task is contained in the artefact "stakeholder requests". The Quranic analyst specifies a requirement

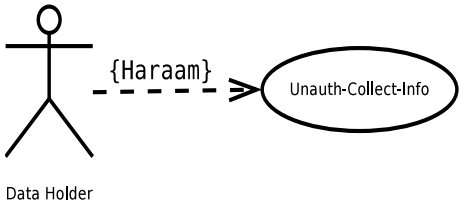

Figure 4.4: *Ahkamic diagram for an unauthorised data collection*

by extending the Quranic *Hukm* of an *Asl* to its corresponding *Far*. We note that *Asl* 1 and *Far* 1 have same *Illah* underneath them. Based on the shared *Illah* between *Asl* 1 and *Far* 1, *Qas* can extend the *Hukm* of *Asl* 1 to *Far* 1. On the basis of shared *Illah* between *Asl* 1 and *Far* 1, we suppose that *Qas* might generate the following requirement.

Requirement for Collect-Info. No data holder X is allowed to collect personal information of any data subject Y until X offers Salaam to Y and X obtains approval of Y

In this requirement, the Arabic saying "*Salaam*" is a required declaration of no-harm by the data holder to data subjects. We note a similar concept in organisations with computer-based systems. These organizations usually seek a declaration from their computer system's users that they will not use the computer systems to harm other people. In technical authentication protocols, the same kind of declaration is also required from the visitor who wants to access a resource (Burrows et al., 1990).

In the iteration of the QuRUP described above, only one privacy requirement is elicited by using the QuRUP. Reiterating the QuRUP elicits more privacy requirements. After requirements have been elicited by using the QuRUP, the Quranic analyst can do further processing on elicited requirements. In the post processing on requirements, the Quranic analyst could remove any inconsistency among requirements. The Quranic analyst may also prioritise these requirements. In this thesis, we limit our work to requirements elicitation only. The refinement of requirements is done in the task "evaluate results" of the RUP. In results evaluation in the RUP, every request is prioritised, and every request has information about what or who is the source of a request because obvious inconsistencies

between requests are removed. In the RUP, while evaluating results, all elicited requests are also presented to customers or users to identify issues that must be addressed. If any issues arise, the members of the RE team address them accordingly. However, in the QuRUP refining requirements occurs in the future. After the refinement work in the QuRUP, all requirements can be modelled back in the artefact "stakeholder requests"; this artefact can be used in other tasks and activities of system development. Although refinement of requirements in detailed form is future work, but in order to evaluate the QuRUP, we will perform a preliminary form of analysis on our elicited requirements. In this preliminary analysis on requirements elicited through the QuRUP, we will eliminate superfluous requirements, remove obvious inconsistencies between requirements, and prioritise elicited requirements.

4.3 The QuRUP vs the RUP

The QuRUP is a process which is proposed to elicit Quranic requirements of Muslim system stakeholders. However, the RUP is a general process used to elicit requirements of any stakeholders including the requirements of Muslim system stakeholders. We do not find any explicit structures in the RUP useful for eliciting Quranic requirements of Muslim system stakeholders. However, to elicit non-religious (non-Quranic) requirements of Muslim system stakeholder, the RUP will probably be a better process.

In the RUP, the task of stakeholder requirements elicitation is contained in the requirements discipline of the RUP. The four steps in this task are "determine sources of requirements", "gather information", "conduct requirements workshops", and "evaluate your results". However, the activity of requirements elicitation in the QuRUP consists of eight tasks. The QuRUP and the RUP share some tasks. However, in the QuRUP some requirements elicitation tasks are absent from the RUP.

For example, in the RUP, during the performance of determine sources of requirements, human and non-human sources of requirements are determined. In the RUP, only the system analyst is responsible for this task, and no additional performer is required. In the RUP, the system analyst identifies individuals who will serve as stakeholder in the RE team. These individuals are identified on the basis of their knowledge, skills, and availability in the project. The system analyst also determines the non-human sources of requirements

such as descriptions of an organisation. In the terminology of the RUP, system analysts along with these individuals are called the "extended project team". This team work together in the requirements elicitation process.

In the QuRUP, during the performance of "determine sources of requirements", human and non-human sources of requirements are determined. In the QuRUP, however, there two analysts, the system analyst and the Quranic analyst. In the performance of this task in QuRUP, the role of system analysts is same as the role of system analysts in the RUP, but the Quranic analyst determines the Islamic sources of requirements such as Quranic explanations and documented opinions of jurists.

The task "elicit *Far*" in the QuRUP is roughly equivalent to the combination of two tasks of the RUP: "gather information" and "conduct requirements worshops". In the RUP, the output of these two tasks is a comprehensive and prioritised set of stakeholders' requests. This output of the RUP is contained an an artefact called "stakeholder requests". In the QuRUP, the output of the task "elicit *Far*" is a *Far* or set of *Far*. These *Far* are not prioritised yet because prioritisation of *Far* is done only after the analysis of the Quranic analyst. In the QuRUP, before any Quranic analysis by the Quranic analyst, the prioritisation of *Far* is not helpful. For example, a user may give a high priority to his demand of wine drinking; however, this demand cannot be a high priority demand in the analysis by the Quranic analyst.

We do not find an equivalent in the RUP to the QuRUP tasks of "elicit *Illah* underneath *Asl* and *Far*", "elicit *Illah* underneath *Far*", and "elicit *Hukm* of *Asl*". The requirement of these tasks in the QuRUP is to get a Quranic *Hukm* on stakeholdes' requests. No such requirement for Quranic *Hukm* on stakeholders' requests is in the RUP. As a result, there is no need for these tasks in the RUP. Moreover, in the QuRUP, the task "prepare iteration plan" is part of requirements elicitation activity. In the RUP, this task is not part of the requirements elicitation activity; however, in the RUP, this is accomplished before doing any of the requirements elicitation tasks. Since in the QuRUP the iteration is limited to requirements elicitation only, we included the task of "prepare iteration plan" within the activity of requirements elicitation. In the RUP, the output of the task "prepare iteration plan" is an input artefact to many activities. Therefore, in the RUP, this task is performed

well before any other activity starts.

4.4 Summary

The QuRUP consists of eight tasks. The output artefact of the QuRUP is a set of requirements. A project manager performs task 1 of the QuRUP. A system analyst performs tasks 2-4 in the QuRUP. Tasks 5-8 in the QuRUP are performed by a Quranic analyst. Requirements elicited through the QuRUP are further analysed to model use cases to build a software system. In a broader sense, for requirements elicitation purpose by using the QuRUP a Quranic interpretation (*Asl*, *Hukm* of *Asl*, and *Illah* underneath *Asl*), and analyses of the system analyst (*Far* with their Illal) are input artefacts to the QuRUP. Quranic-compliant cases are the output artefacts of the QuRUP. In the next chapter, we indicate the use of the QuRUP to elicit more privacy requirements by analysing various activities in the PIdM.

CHAPTER 5

Analysis of the PIdM

If Allah guides a man through your help, it is better (for you) than red camels (Prophet Muhammad)

Everything has it's tax, and the tax of knowledge is to teach others (Imam Ali)

We propose the QuRUP for a duly diligent response to the Quranic concerns of Muslim system stakeholders. The Quranic concerns denote the fears of Muslims of their involvement in an activity that is against the injunction of the Quran and their desires to be involved in a system activity that is harmonious to the injunctions of the Quran. To respond appropriately to the concerns of Muslim system stakeholders, system engineers must elicit the requirements of these stakeholder.

We apply the QuRUP on the PIdM to indicate how requirements could be elicited with due diligence. In analysing the PIdM, our focus is on privacy requirements of Muslim system stakeholders. We argue that other types of requirements which express the concerns of Muslim system stakeholders can also be elicited by using the QuRUP.

To elicit requirements of Muslim system stakeholders, in Chapter 4 we explain our

proposed process of requirements elicitation, i.e the QuRUP. In an application of the QuRUP for requirements elicitation in software systems, we use Quranic *Ahkam* as a source for these requirements. In Chapter 3, we explain Quranic *Ahkam* which constitute the DoCoMo. The DoCoMo is a Quranic private sphere which we constitute by combining domestic privacy-related *Ahkam*, people's communication-related Quranic *Ahkam*, and modesty-related *Ahkam*.

We use the Quranic *Ahkam* of the DoCoMo as a source for eliciting privacy requirements in the PIdM. By analysing the PIdM, we indicate how the QuRUP can be used to identify privacy requirements on the stakeholders of the PIdM. We use these elicited requirements to describe the four groups of information privacy activities proposed by Solove (2006). The four groups of activities proposed by Solove (2006) are information collection, information processing, information dissemination, and invasion. These four group of activities have multiple subgroups of activities. We assume that in applying the QuRUP for privacy requirements elicitation, the system analyst might use Solove's classification as an input to the QuRUP. After applying the QuRUP, privacy requirements are generated which correspond to these four groups of activities, where every privacy requirement would regulate an activity or a set of activities.

In the analysis of the PIdM, every elicited privacy requirement falls within one of the five types of *Ahkam*. These five types of *Ahkam* specify *Haraam* actions, *Waajib* actions, *Mandub* actions, *Makruh* actions, and *Mubah* actions. We use these five Ahkamic values in the Ahkamic diagram to denote the relationship between actor and *Far* constructs of the Ahkamic diagram.

In eliciting Quranic privacy requirements, we do not present the analysis of the complete system of the PIdM. Instead, we present the analysis on the initial phase of obtaining a CNIC. In analysing the initial phase of the PIdM, we indicate how the QuRUP might be used to elicit privacy requirements related to information collection activities, information processing activities, information dissemination activities, and information invasion activities.

In Section 5.1 of this chapter, we indicate how the QuRUP can be applied to the information collection activities of the PIdM. In Section 5.2, we indicate an application of

the QuRUP on information processing activities of the PIdM. In Section 5.3, we show an application of the QuRUP on the information dissemination activities of the PIdM. Section 5.4 of this chapter deals with the task of eliciting privacy requirements from the invasive activities in the initial phase of the PIdM, and this task is followed by our discussion on elicited privacy requirements.

5.1 Information collection

Information collection activities affect people's privacy. For eliciting privacy requirements for this group of activities in the PIdM, we assume that *Sam*, the system analyst of the PIdM, starts with constructing various scenarios by which the data holder of the PIdM collects personal information from data subjects. We also assume that iteration plan and resources in the PIdM are the same during each iteration of the QuRUP. In Chapter 4, the iteration plan was only for requirements collection activities, but in this chapter the iteration plan also includes information processing, information dissemination, and invasion. We note that surveillance, extortion, prying, and no-Salaam are four types of information collection activities. Solove (2006) also mentions surveillance, extortion, and prying as information collection invasions. Below we indicate how an RE team might apply the QuRUP to elicit privacy requirements for each of the four types of information collection activities in the PIdM.

5.1.1 The QuRUP on information collection by surveillance

Generally, surveillance is the process of monitoring, listening, or recording an individual's activities. Surveillance is a form of an involuntary gathering of information, and it is often carried out surreptitiously. It is possible that the data holder of the PIdM may collect personal information of data subjects through surveillance. Surveillance includes monitoring and recording other people's personal information. There could be various ways of capturing people's personal information through surveillance. For simplicity, we discuss only one scenario that the data holder collects personal information of data subjects by surreptitiously monitoring digital records on computer systems of data subjects. This is covert surveillance. Below we indicate how the QuRUP might be applied to discover a Quranic requirement for this scenario of covert surveillance.

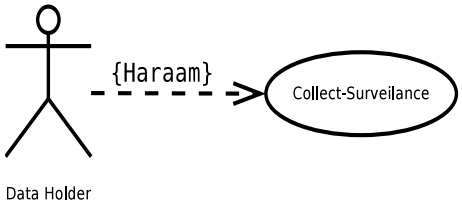

Figure 5.1: *Ahkamic diagram for data collection by surveillance*

1. Elicitation of Far

   This task is Sam's responsibility. *Sam* will look for modelling two constructs of the Ahkamic diagram: Far and actor. To elicit the Far construct for an information collection activity in the PIdM, we assume that *Sam* carries on from Far Collect-Info elicited in the previous Chapter. *Sam* might use Collect-Info elicited before as an input artefact to the QuRUP. Far Collect-Info is "A data holder X collects personal information of a data subject Y ". It is possible that Collect-Info might be carried out by surveillance.

   We assume that the data holder may wish to collect personal information of data subjects through surveillance. In the PIdM, actually its data holder does not collect people's personal information through surveillance. Considering the possibility that the data holder may wish to collect personal information of data subjects by the process of surveillance, we indicate how the QuRUP might be used to specify a requirement for this particular behaviour of the data holder. For Quranic reasoning purposes, the scenario of information collection by surveillance can be considered as an action of the data holder. Therefore, *Sam* might construct this action of the data holder as a Far which is listed below.

   Far Collect-Surveillance. A data holder X collects by surveillance any personal information of a data subject Y

   Collect-Surveillance and its actor are modelled in an Ahkamic diagram shown in Figure 5.1. The third construct of this diagram will be determined by *Qas*. This construct is a *Hukm* specified for Collect-Surveillance. This *Hukm* will be an extension of an *Asl* which is relevant to Collect-Surveillance.

2. Elicitation of Illah underneath Far

   This task is also performed by *Sam*. *Illah* underneath Far is the effective cause which renders Far for a Quranic *Hukm*. Collect-Surveillance is an input artefact to this task of the QuRUP. For this Far, we identify *Illah* by the process of accomplishment of this Far. This Far is accomplished through surveillance, and by surveillance one's computer system is invaded, we say that *Illah* underneath Collect-Surveillance is "invasion of the private sphere of data subjects". This is because we consider a computer system which contains people's personal digital records as part of people's private sphere. We assume that *Sam* might also elicit this *Illah* for Collect-Surveillance. Below we list this *Illah*.

   Illah underneath Collect-Surveillance. Invasion of one's private sphere

3. Elicitation of Asl

   This task is performed by *Qas*, the Quranic analyst of the PIdM. Collect-Surveillance along with its *Illah* are input artefacts to this task of the QuRUP. We assume that *Qas* might elicit the following *Asl* from the Quranic verse 24:27, previously explained at page 56 .

   Asl Entry-Unauth. A person X enters without any authorisation in the house of a person Y

   We argue that Entry-Unauth is relevant to Collect-Surveillance. In the case of Collect-Surveillance, data holders collect personal information of data subjects without any authorisation from data subjects. Similarly, in Entry-Unauth, a visitor enters someone else's house without any approval from the inhabitants of the house. In both cases, two parties are involved. One party is the intruder, and the other party involved is an individual whose privacy is being invaded by the first party. The private sphere in Entry-Unauth is defined relative to a house, and the private sphere in Collect-Surveillance is one's computer system which holds personal information.

   In both cases, we can imagine that there is a wall between the private sphere and the public sphere, or at least an intent from data subjects to have a wall. In the case of Entry-Unauth, the presence of a house indicates that there is a wall between public and private spheres constituted by the house. However, it is worth mentioning that

in Entry-Unauth the wall between the public and the private sphere is not necessarily the literal wall of an actual house. Instead, the wall between the public and the private domestic sphere is metaphorical wall which secures the house from any unwelcome intrusions. According to the Quran, the wall between one's domestic private sphere and public sphere can extend far beyond the actual boundaries or walls of a house. In the case of Collect-Surveillance, the wall between the private and the public sphere can be considered as the interface of a computer system. Someone who crosses this interface without any authorisation would be called as an intruder. Similarly, in Entry-Unauth when a visitor enters in a house without any authorisation from the inhabitants of the house, the visitor would be recognised as an intruder.

Based on the aforementioned similarities between Entry-Unauth and Collect-Surveillance, we conclude that Entry-Unauth is a relevant case to Collect-Surveillance. Therefore, information collection by surveillance of other people's computer systems is roughly equivalent to entering other people's houses without the approval of house's inmates. Based on the similarity of Entry-Unauth and Collect-Surveillance, by using Qiyas, the *Hukm* of Entry-Unauth can be extended for Collect-Surveillance. Below, the activity of eliciting *Hukm* for Entry-Unauth is discussed.

4. Elicitation of Hukm for Asl

   Qas is responsible for performing this task of the QuRUP. *Asl* is an input artefact, and a Quranic *Hukm* for this *Asl* is an output artefact of this task. We note that in the Quranic verse 24:27, the *Hukm* for Entry-Unauth is very clear. Therefore *Qas* might also capture this clear *Hukm*. The *Hukm* being conveyed through Entry-Unauth is listed below.

   Hukm for Entry-Unauth. No person X without authorisation is allowed to enter the house of person Y

5. Elicitation of Illah underneath Asl

   Qas is responsible for the performance of this task of the QuRUP. An *Asl* is an input artefact to this task, and an *Illah* underneath the *Asl* is an output artefact of this task. We play the role of the Quranic analyst and identify *Illah* underneath Entry-Unauth. Based on our reading of the Quranic explanation of Maududi, we identify an *Illah*

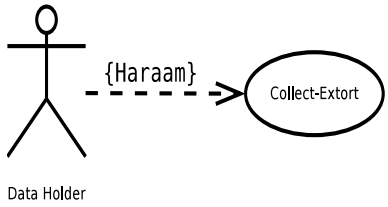

Figure 5.2: *Ahkamic diagram of data collection by extortion*

underneath Entry-Unauth. We suppose that *Qas* might also elicit the same *Illah* for Collect-Surveillance, and this *Illah* is listed below.

Illah underneath Entry-Unauth. Invasion of one's private sphere

6. Specify requirement

   Qas performs this task. Based on the shared *Illah* between Entry-Unauth and Collect-Surveillance identified above, we assume that *Qas* might extend *Hukm* of Entry-Unauth to specify *Hukm* for Collect-Surveillance. The *Hukm* for Collect-Surveillance is depicted in the Ahkamic diagram 5.1. After eliciting *Hukm* of Collect-Surveillance, *Qas* might conclude the following privacy requirement.

   Requirement for Collect-Surveillance. No data holder X is allowed to collect by surveillance any personal information of data subject Y

5.1.2 The QuRUP on information collection by extortion

Now we indicate the application of the QuRUP on another scenario of information collection by extortion. In applying the QuRUP to this scenario of information collection, iteration plan and resources are the same as what has been specified for other iterations of the QuRUP. Below the application of the QuRUP on the scenario of information collection by extortion is explained.

1. Elicitation of Far

   In this scenario, the data holder collects personal information of data subject by keeping them under duress. Collect-Extort is constructed on the basis of this scenario of information collection. Collect-Extort and its actor are depicted in Figure 5.2. In the case of extortion, the data subject is compelled (by threat of violence, *e. g.* an

interrogation, or some other adverse outcome, such as a threat to a loved one) to provide information to the data holder. Extortion is similar to surveillance in that in both cases information collection is without any permission of data subjects. However, information collection by surveillance is different from information collection by extortion. In the case of surveillance the data subject is unaware that his personal information is being collected, whereas in the case of extortion the data subject is aware that their information is being collected. From the scenario of information collection by extortion, we assume that *Sam* might construct the following Far.

Collect-Extort. A data holder X collects by distortion any personal information from a data subject Y

2. Elicitation of Illah underneath Far

   Collect-Extort is an input artefact to this task of the QuRUP. *Sam* determines *Illah* underneath Collect-Extort. The *Illah* underneath Collect-Extort is listed below.

   Illah underneath Collect-Extort. Extortion

3. Elicitation of Asl

   Qas is responsible for this task of the QuRUP. The following *Asl* for Collect-Extort is elicited.

   Obtain-Extort. A person X obtains anything by extortion from a person Y

   This *Asl* is elicited on the basis of the Quranic verse 2:188. In this verse, believers are commanded to not usurp one another's property by unlawful means. Here is the Quranic verse.

   > Do not usurp one another's property by unjust means nor offer it to the judges so that you may devour knowingly and unjustly a portion of the goods of others (Quran 2:188)

   There is further support on the prohibition for extorting other people's property in the following *Hadith* which we quote from the work of Amin et al. (2009).

> Do not be envious of one another; do not artificially inflate prices against one another; do not hate one another; do not shun one another; and do not undercut one another in business transactions; and be as fellow-brothers and servants of Allah. A Muslim is the brother of a Muslim. He neither oppresses him nor humiliates him nor looks down upon him. Piety is here - and he pointed to his chest three times. It is evil enough for a Muslim to hold his brother Muslim in contempt. All things of a Muslim are inviolable for another Muslim: his blood, his property and his honour (Amin et al., 2009).

4. Elicitation of Illah underneath Asl

   Qas performs this activity. It is very clear from the Quranic verse above that "extortion" is an *Illah* under the Obtain-Extort which is elicited from this verse. We list this *Illah* below.

   Illah underneath Obtain-Extort. Extortion

5. Elicitation of Hukm for Asl

   Qas performs this task. On the basis of the Quranic prohibition on extortion as mentioned in the Quranic verse 2:188, we specify the following *Hukm* for Obtain-Extort. We assume that *Qas* would also elicit the same *Hukm* for Obtain-Extort.

   Hukm for Obtain-Extort. No person X is allowed to obtain anything by extortion from person Y

6. Specify requirement

   Qas is responsible for the performance of this task of the QuRUP. Because of the shared *Illah* between Obtain-Extort and Collect-Extort, the *Hukm* of Obtain-Extort can be extended to Collect-Extort. The *Hukm* for Collect-Extort is therefore a prohibition which is depicted in the Ahkamic diagram of Figure 5.2. From the Quranic *Hukm* for Collect-Extort, *Qas* might conclude the following privacy requirement.

   Requirement for Collect-Extort. No data holder X is allowed to extort any data subject Y to obtain their personal information

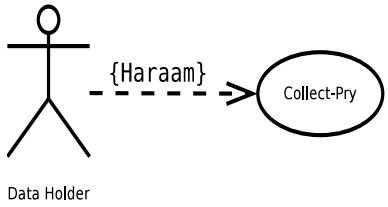

Figure 5.3: *Ahkamic diagram of data collection by prying*

5.1.3 The QuRUP on information collection by prying

Prying is another scenario of data collection. In the case of information collection by prying, the data holder collects personal information of data subjects by searching their digital records. Prying could also be done by asking direct or indirect questions in a routine talk with data subjects. The difference between prying by searching and prying by asking questions is that in the former scenario, the data subject is not interacting at all, while in the later one, the data subject is also involved. The essence in both scenarios is the same the data holder is maliciously obtaining personal information of data subjects. Below we indicate how the QuRUP might be applied to discover Quranic requirement for the scenario of prying.

1. Elicitation of Far

   In this task *Sam* identifies two constructs of the Ahkamic diagram. These two constructs are *Far* and actor. From the scenario of prying discussed above, *Sam* might elicit the following Far.

   Collect-Pry. A data holder X pries to obtain personal information of data subject Y

   Collect-Pry and its actor (data holder) are depicted in the Ahkamic diagram. Figure 5.3 contains this Ahkamic diagram of Collect-Pry and its actor.

2. Elicitation of Illah underneath Far

   This task is performed by *Sam*. *Illah* underneath Far is the effective cause which renders Far for a Quranic *Hukm*. Collect-Pry is an input artefact to this task of the QuRUP. We note that the successful completion of Far is likely to cause an emotional,

mental, or physical injury to data subject. It could also cause mental uneasiness to data subjects who information has been collected. Solove (2006) considers the mental uneasiness of people as an injury to them. Keeping in view the consequences of the successful completion of Collect-Pry, *Sam* might elicit the following *Illah* underneath Collect-Pry.

Illah underneath Collect-Pry. Personal injury

3. Elicitation of Asl

   Collect-Pry along with its *Illah* are input artefacts to this task of the QuRUP. We note that the following verse of the Quran regulate spying and prying people's affairs.

   > O you who have believed, avoid much suspicion, for some suspicions are sins. Do not spy, nor should any one backbite the other. Is there any among you who would like to eat the flesh of his dead brother? Nay, you yourselves abhor it. Fear Allah, for Allah is Acceptor of repentance and All-Merciful (Quran 49:12).

   From the above verse of the Quran, *Qas* might elicit the following *Asl* which is relevant to the input Far.

   Asl No-Pry. A person X pries another person Y

   In explaining the Quranic verse 49:12, Maududi mentions that searching other people's secrets whether this is done because of suspicion, or for causing harm to somebody with an evil intention, or for satisfying one's own curiosity, it is forbidden by the *Shariah* in every case. He further mentions that the Quran prohibits prying into conditions and affairs of other people. We note that the essence of Maududi's explanation is that every type of search for any kind of secret for any purpose is not allowed in the *Shariah*. Collect-Pry is one form of prying which is for personal information collection. However, No-Pry deal with every kind of prying. Therefore, we can say that No-Pry fully covers Collect-Pry.

4. Elicitation of Hukm for Asl

   Qas performs this task of the QuRUP. In the Quranic verse 49:12, the *Hukm* for prying

is quite clear. The Quranic prohibition on prying other people is listed below as an *Hukm* of No-Pry.

Hukm for No-Pry. No one is allowed to spy other people

5. Elicitation of Illah underneath Asl

   Qas is responsible for the performance of this task of the QuRUP. Maududi mentions that prying into other people's affairs is the evil which is not only a sin in itself but it also corrupts a society. We infer from Maududi's explanation that prying could also damage an individual which is a component of a society. We therefore consider "personal injury or damage" as one of the *Ilal* underneath the prohibition of prying. We assume that *Qas* might also elicit the following *Illah* underneath No-Pry.

   Illah underneath No-Pry. Personal injury

6. Specify requirement

   No-Pry and Collect-Pry along with their Ilal are input artefacts to this task of the QuRUP. Based on the shared *Illah* between No-Pry and Collect-Pry identified above, the *Hukm* of No-Pry can be applied to Collect-Pry. The *Hukm* of Collect-Pry is depicted in Figure 5.3. From the Quranic *Hukm* for Collect-Pry, the following privacy requirement is concluded.

   Requirement for Collect-Pry. No data holder X is allowed to pry for obtaining personal information of a data subject Y

5.1.4 The QuRUP on information collection by no-Salaam

In addition to surveillance, extortion, and prying the no-Salaam is a information collection scenario. Below we discuss this scenario and indicate how the QuRUP might be applied to define a Quranic requirement for this scenario.

1. Elicitation of Far

   In this case of personal information collection, the data holder collects personal information of data subjects without offering *Salaam* to data subjects. Like other Far and their actors, no-Salaam and its actor (data holder) can be represented in an Ahkamic

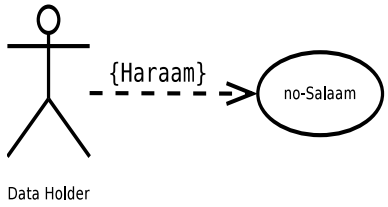

Figure 5.4: *Ahkamic diagram for data collection by no-Salaam scenario*

diagram. The no-Salaam scenario might be a data collection in which there is no compulsion (as in Collect-Extort), and in which the data subject was notified so that it is clearly distinct from Collect-Surveillance; however, the data subject's permission was either sought incorrectly or the permission was not granted. For an example, of no-Salaam entrance someone knocks on the door, yells, "let me in", and then runs past the doorkeeper without waiting for an answer. Alternatively, if someone asks for permission and permission is granted, then enters the house without offering *Salaam* to those within. This is also an example of no-Salaam entrance. From these no-Salaam scenarios, we assume that *Sam* might construct the following Far.

Far no-Salaam. A data holder X collects any personal information from a data subject Y without offering any Salaam to Y

This Far and its actor are modelled in Figure 5.4. In this figure, we model "no-Salaam" data collection scenario by a use case construct. The scenario no-Salaam represents a case of information collection by a data holder without prior offering *Salaam* to data subjects. In Figure 5.4, the data holder is modelled by an actor construct. In this figure, the relationship between the actor and use case construct specifies the *Hukm* on data holder for this scenario.

2. Elicitation of Illah underneath Far

   This is another of *Sam*'s tasks. A no-Salaam is an input artefact to this task of the QuRUP. As mentioned before, offering *Salaam* indicates that the one who offered *Salaam* is not an attacker, and he would not harm the person to whom he has offered *Salaam*. However, if someone enters someone else's house without offering *Salaam*, then the householder might feel uncomfortable in the presence of this visitor. The

household might consider the visitor who has not offered *Salaam* an attacker. We therefore say that discomfort of members of the household is one of the *Ilal* underneath the scenario of no-Salaam entering the house. We assume that *Sam* might also elicit the following *Illah* for no-Salaam.

Illah underneath no-Salaam. Discomfort

3. Elicitation of Asl

   From the Quranic domestic *Ahkam* specified in the Quranic verse 24:27, *Qas* might elicit the following *Asl* which is relevant to no-Salaam.

   Asl no-Salaam-Entry. A person X enters the house of another person Y without offering Salaam to Y

4. Elicitation of Hukm for Asl

   Qas performs this task of the QuRUP. The Quranic verse 24:27 clearly prohibits entering other people's houses without *Salaam*. Therefore, *Qas* would also use this *Hukm* for the QuRUP; as listed below.

   Hukm for no-Salaam-Entry. No person X is allowed to enter the house of another person Y without offering Salaam to Y

5. Elicitation of Illah underneath Asl

   Qas is the performer of this task. We note that neither the Quranic text nor the explanation by Maududi explicitly specifies an *Illah* underneath the requirement of offering *Salaam* before entering some one else's house. However, from the meaning of the Arabic word *Salaam*, we tentatively conclude that discomfort to members of the household is an *Hikmah* underneath the *Illah* of no-Salaam-Entry. We further use this *Hikmah* as an *Illah* underneath no-Salaam-Entry. In the *Shariah*, *Hikmah* of an *Asl* is sometimes used as an *Illah* of this *Asl*. We remind readers that the Arabic term *Hikmah* is the effective cause underneath an *Illah*. We assume that *Qas* would also elicit the following *Illah* underneath no-Salaam-Entry.

Illah underneath no-Salaam-Entry. Discomfort

6. Specify requirement

   Based on a shared *Illah* between no-Salaam-Entry and no-Salaam as identified above, the *Hukm* of no-Salaam-Entry can be extended to specify the *Hukm* of no-Salaam. The *Hukm* for no-Salaam which is a prohibition can be depicted in an Ahkamic diagram to denote that the performance of no-Salaam in information collection is an *Haraam* act. From the Quranic *Hukm* for no-Salaam, *Qas* might conclude the following privacy requirement.

   Requirement for no-Salaam. No data holder X is allowed to obtain personal information of a data subject Y without offering Salaam to Y

So far the use of QuRUP on restricted personal information is indicated. It was assumed that either data subjects had either protected their information or at least they had an intent to protect their personal information. The issue of publicly available information arises: how does the QuRUP counters with requirements elicitation for people's personal information that they had made publicly available on their web-pages, for example?

5.1.5 The QuRUP on publicly available information

People often make some of their personal information publicly available. For example, on their web pages they publicly provide their names, email address, office address, and publication. We note that this provision is often very useful to other people as well to the owner of such information. People often benefit by using this publicly available information. Below we indicate the use of QuRUP to elicit requirements about the collection of publicly available personal information.

1. Elicitation of Far

   This time *Sam* performs this task. Based on the above scenario, we assume that *Sam* might elicit the following Far for the purpose of applying the QuRUP on publicly available information.

   Far Collect-pubInfo. A data holder X collects publicly available personal information of a data subject Y

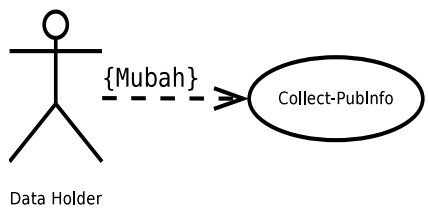

Figure 5.5: *Ahkamic diagram for collecting publicly available data*

Collect-pubInfo and its actor (data holder) are depicted in Figure 5.5 of the Ahkamic diagram of Collect-pubInfo and its actor.

2. Elicitation of Illah underneath Far

   Sam again performs this task. Collect-pubInfo is an input artefact to this task of the QuRUP. We do not see any harm in the accomplishment of Collect-pubInfo. In terms of privacy violations, we also do not see any privacy violation of data subjects on the completion of Collect-pubInfo because they have made their data publicly availably. *Sam* might also conclude no privacy violation in accomplishing Collect-pubInfo. Below we list this no privacy violation as an *Illah* underneath Collect-pubInfo.

   Illah underneath Collect-pubInfo. No privacy violation

3. Elicitation of Asl

   We use Collect-pubInfo along with its *Illah* as input artefacts to this task of the QuRUP. We assume that *Qas* might elicit the following *Asl* which is relevant to Collect-pubInfo.

   Entry-pubSpace. Entering uninhabited houses

   This *Asl* is elicited from the Quranic verse 24:29 which reveals that entry is not prohibited to such buildings.

   > There is, however, no harm if you enter houses which are not dwelling places, but contain something useful for you; Allah knows what you disclose and what you conceal (Quran 24:29).

From this verse, Maududi concludes that it is *Mubah* to enter a building, such as a shop, hotel, or guest house, which is generally open to all people. We believe that Entry-pubSpace is relevant to Collect-pubInfo. Obtaining publicly available information about people is arguably similar to entering a public place like a shop or a restaurant.

4. Elicitation of Hukm for Asl

   This is another task of *Qas*. The *Hukm* for Entry-pubSpace in the Quranic verse 24:29 is very clear.

   Hukm for Entry-pubSpace. Every person X is allowed to enter an uninhabited house

5. Elicitation of Illah underneath Asl

   Qas is responsible for the performance of this task. As mentioned by Maududi, one of the reasons behind permitting people to enter uninhabited houses is that this entrance is not an invasion of anyone's privacy, and also on entering a house the visitor may get some thing benefit. From Maududi's explanation, we conclude that *Qas* might elicit the following *Illah* underneath Entry-pubSpace.

   Illah underneath Entry-pubSpace. No privacy violation

6. Specify requirement

   Based on a shared *Illah* between Entry-pubSpace and Collect-pubInfo identified above, the *Hukm* of Entry-pubSpace can be extended to specify *Hukm* for Collect-pubInfo. From the Quranic *Hukm* for Collect-pubInfo, *Qas* might conclude the following privacy requirement.

   Requirement for Collect-pubInfo. A person X is allowed to collect publicly available personal information of a data subject Y

In the foregoing application of the QuRUP, we elicit requirements which correspond to various information collection activities in the PIdM. We note that these requirements restrict or regulate the flow of data from its actual owners to data holders who often provide some

services to data subjects. In eliciting these requirements, we assume that people's data is in their own control. These requirements regulate the flow of data from their owners to data holders. When people's personal information or data goes to the hands of data holders, some protection of the privacy of the owners of this data is necessary. Below we use the QuRUP for eliciting requirements on data holders, data subjects, and on other people in the process of processing people's personal data.

5.2 Information processing

In the previous section, we indicated how the QuRUP might be used to elicit privacy requirements by analysing various information collection activities. Solove (2006) indicates that there are some Information processing activities from which privacy violations may occur. Information processing activities deal with handling of already collected data. In this section, we indicate the use the QuRUP in eliciting information processing related privacy requirements.

Solove (2006) mentions "insecurity" as one of the major causes of privacy violations. Solove (2006) also mentions that insecurity is a problem caused by the way our information is handled and protected. Solove (2006) further mentions that insecurity exposes people to potential future harm such as identity theft is a result of insecurity. Because of the insecurity of data, people's personal information could be polluted by attackers. Distortion which is the dissemination of false information about a person is therefore an aftermath of insecurity. Solove (2006) himself writes "glitches, security lapses, abuses, and illicit uses of personal information all fall into this category [insecurity]" (Solove, 2006).

data holders may leave people's personal information unprotected or inadequately protected. Inadequately protected data or unprotected data is one form of insecure data. Leaving people's personal data insecure allows attackers to manipulate or steal this data. Eventually this could harm the owner of this information. Therefore, leaving people's personal information insecure is a cognisable injury to the people to whom this information belongs.

We use the above information processing scenarios for privacy requirements elicitation. We use these scenarios as an input to the QuRUP. Below we explain our use of the QuRUP for eliciting requirements arising from this scenarios.

1. Elicitation of Far

   Insecurity of data holders' personal information exposes them to potential harm. Insecure data facilitate an attacker to pollute the data or to steal the data. From this scenario, we assume that *Sam* might construct a Far which is listed below.

   Far Insecure-Info. A data holder X does not secure personal information of a data subject Y

2. Elicitation of Illah underneath Far

   We say that without securing any data, this data would be insecure. Insecurity of data can cause future harm. Solove (2006) even considers insecurity itself as cognisable injury. The essence in considering insecurity as a cognisable injury is that by insecurity of data one's privacy is at stake. We therefore consider privacy invasion as an effective cause underneath insecurity. We assume that *Sam* might also elicit privacy invasion as an *Illah* underneath Insecure-Info.

   Illah underneath Insecure-Info. Privacy invasion

3. Elicitation of Asl

   The Quran reveals that it is *Waajib* for believing men and women to restrain their gazes and guard the private parts of their bodies. This is evident from the following verses of the Quran.

   > And O Prophet, enjoin the Believing men to restrain their gaze and guard their private parts. This is a more righteous way for them: Allah has knowledge of what they do. O Prophet, enjoin the Believing women to restrain their gaze and guard their private parts ... (Quran 24:30-31).

   For specifying an *Asl*, we use the requirements in the above verses of Quran. From these Quranic verses, we assume *Qas* might elicit the following *Asl*.

   Asl Control-Gaze. A person X restrains his gazes from watching the private body parts of a person Y

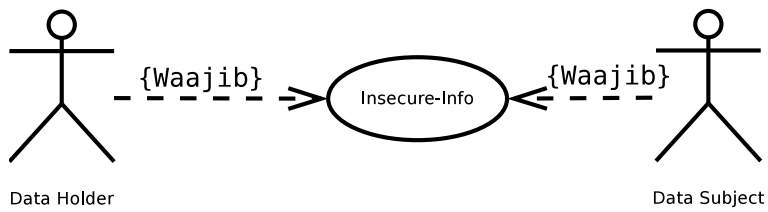

Figure 5.6: *Ahkamic diagram for information insecurity*

4. Elicitation of Illah underneath Asl

   Maududi interprets "restraining gazes" to mean protection of other's privacy, and "guarding private parts" is protection of one's own privacy. It is clear from these verses that guarding private parts is *Waajib* for both men and women. Restraining gazes is also *Waajib* on believers for the protection of other's privacy. Therefore, one of the Ilal underneath Control-Gaze is "protection of other people's privacy". We list this *Illah* of Control-Gaze.

   Illah underneath Control-Gaze. Protection of privacy

5. Elicitation of Hukm for Asl

   From the Quranic verses 24:30-31, the following *Hukm* is very clear.

   Hukm for Control-Gaze. No person X is allowed to look at the private body parts of a person Y

6. Specify requirement

   Based on a shared *Illah* between Control-Gaze and Insecure-Info identified above, the *Hukm* of Control-Gaze can be extended specify *Hukm* for Insecure-Info. From the Quranic *Hukm* for Insecure-Info, *Qas* might conclude the following privacy requirement.

   Requirement for Insecure-Info. A data holder X must secure personal information of a data subject Y

Insecure-Info, its actor, and the relationship between Insecure-Info and its actor are depicted in Ahkamic diagram 5.6. The privacy requirement Insecure-Info applies to both data subjects and data holders. This Ahkamic diagram indicates that data holders and data

subjects must secure their own personal information. Also, data holders must secure the personal information that they collect from data subjects. There is further support to requirements Insecure-Info in an *Hadith* which is narrated by Imam Ali. Imam Ali (*Karam ullah Wajhu*) narrates that every believer has thirty obligations over his brother in faith and to guard his secrets is one among these thirty obligations. According to Shaikh Rafat Najm, this *Hadith* is in Wasa'l alshe'a ('al albait)—Alhur alma'ameli Volume 21 Page. 212.

5.3 Information dissemination

In the previous two sections, we indicated how the QuRUP might be applied to elicit various information collection and information processing requirements. Now we indicate the use of the QuRUP in elicitation of Quranic requirements related to information dissemination. In the PIdM , its data holder has personal information of data subjects. The data holder of the PIdM may disclose this personal information to others. However, disclosure of personal information can harm data subjects. To deal with the disclosure of people's personal information in the PIdM, we indicate the use of the QuRUP to elicit requirements from the Quran. System developers can use these requirements in order to obviate any harm from the disclosure of people's personal information. Below we show an application of the QuRUP for this purpose.

1. Elicitation of Far

   We consider the possibility that data holders may disclose personal information of data subjects. From this scenario, *Sam* might construct the following Far.

   Far Reveal-Info. A data holder X discloses personal information of a data subject Y

   Reveal-Info, its actor, and the relationship between Reveal-Info and its actor are depicted in an Ahkamic diagram 5.7. In this figure, we model two actors: data holder and data subject. Modelling these two actors with one use-case construct (Disclos-Info) indicates that Disclos-Info has relationship with data holder and data subject. Although, every data subject is a data holder of his/her personal information but to emphasise the Quranic requirement on data subjects, we explicitly model a data subject actor in this Ahkamic diagram.

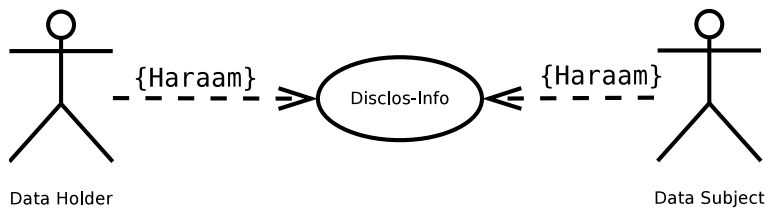

Figure 5.7: *Ahkamic diagram for information disclosure*

2. Elicitation of Illah underneath Far

   The disclosure of personal information belonging to data subjects by their data holders may harm data subjects. Even if the disclosure does not cause any apparent harm to data subjects, the disclosure could cause mental uneasiness to data subjects. Solove (2006) considers people's mental uneasiness as an injury. We consider mental uneasiness as an *Illah* underneath Disclos-Info. We list this *Illah* as below.

   Illah underneath Reveal-Info. Mental uneasiness

3. Elicitation of Asl

   From the following verses of the Quran, we elicit an *Asl* which is relevant to Reveal-Info.

   > (And this also is noteworthy that) the Prophet had confided a matter to a wife in secret. Then, when she disclosed the secret (to another), and Allah informed the Prophet (of the disclosure of the secret), the Prophet made known (to the wife) part of it and overlooked part of it. So when the Prophet told her (of the disclosure), she asked, "Who informed you of this?" The Prophet said, "I was informed by Him Who knows everything and is All-Aware." If you both (women) repent to Allah, (it is better for you), for your hearts have swerved from the right path and if you supported each other against the Prophet, you should know that Allah is his Protector, and after Him Gabriel and the righteous believers and the angels are his companions and helpers. It may well be that if the Prophet divorces all of you, Allah will give him in your place better wives, who

> are true Muslims, who are believing and obedient, penitent, worshipping, and given to fasting, be they previously married or virgins (Quran 66:3-5).

In these verses, two wives of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) disclosed a secret. They were advised to repent to Allah. Additionally, they were warned of dire consequences (divorce), if they chose not to repent. Maududi states that Allah requires people to refrain from disclosing other people's secrets. We identify this requirement as *Asl*, because, we use this requirement as a source for deriving requirements for the PIdM. In this *Asl*, there are two types of actors involved. The Type 1 actor possesses a secret of the Type 2 actor. The requirement is on the future actions of the Type 1 actor. We assume that *Qas* might also elicit the same *Asl* as listed below.

Asl Disclos-Secret. A person X discloses a secret of another person Y

4. Elicitation of Illah underneath Asl

   According to Maududi, the *Illah* underneath the reprimand and the demand for repentance described in the above verse is the disclosure of a secret. Maududi further mentions that the disclosure of the secret mentioned in the Quranic verses 66:3-5 caused mental uneasiness to Prophet Muhammad (*Sallallahu Alaihi wa Sallam*). In the explanation of these verses, Maududi insists of non-disclosure of other people's secrets. One of the consequences of disclosing people's secrets is their mental uneasiness. Avoiding mental uneasiness of people can be considered as an *Hikmah* of regulating the disclosure of people's secrets. For the purpose of this thesis, we consider this *Hikmah* as an *Illah* underneath the Quranic verses 66:3-5. Below we list this *Illah*.

   Illah underneath Disclos-Secret. Mental uneasiness

5. Elicitation of *Hukm* for Asl

   In the Quranic verses 66:3-5, the *Hukm* for Disclos-Secret is clearly mentioned. We list this *Hukm* as below.

Hukm for Disclos-Secret. No person X is allowed to disclose a secret of a person Y

6. Specification of Hukm for Far

   Based on a shared *Illah* between Disclos-Secret and Reveal-Info identified above, the *Hukm* of Disclos-Secret can be extended to specify *Hukm* for Reveal-Info. From the Quranic *Hukm* for Reveal-Info, *Qas* might conclude the following privacy requirement.

   Requirement for Reveal-Info. No data holder X is allowed to disclose personal information of a person Y

If we analyse the information dissemination scenario, it is possible that the information disclosure may not cause any mental uneasiness to data subjects. Or data subjects could be unaware of the disclosure of their personal information by data holders. The question arises that in this situation, is disclosure of personal information permitted?. We argue from the Quranic verse 24:8 that data holders must not disclose anyone's personal information irrespective of the consequences of this disclosure. Below we quote this Quranic verse to distinguish a feature of Muslims, that they faithfully observe their trusts and their covenants.

> [Muslims] are true to their trusts and their promises (Quran 23:8).

In explaining the above verse, Maududi mentions that one is not allowed to disclose any secret about other people even if this disclosure does not cause any injury or harm to the one who originally confided the secret. In the following *Hadith* that we quote from the Quranic explanation of Maududi, there is further support to not disclose people's trusts or personal information. Maududi mentions that Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) is reported to have said: "the one who does not fulfil the terms of his trust, has no Faith, and the one who does not keep promises and pledges has no Islam".

When data holders collect personal information, they have an implicit promise to not disclose this information to any third party. We conclude that disclosure of any type of secret about other people is not permitted, irrespective of its possible consequences.

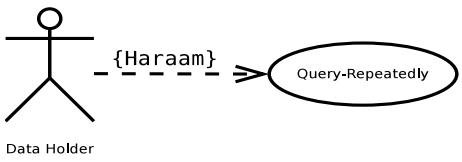

Figure 5.8: *Ahkamic diagram for repeated attempts to get data*

5.4 Information invasion

In privacy harm during information collection, information processing, and information dissemination, personal data moves further away from the control of the people. However, in privacy harm during information invasions, instead of the progression away from the people, invasions progress towards the people.

Solove (2006) mentions that intrusion which is a form of invasion interrupts one's activities through the unwanted presence or activities of another person. He further states that "intrusion need not involve spatial incursions: spam, junk mail, junk faxes, and telemarketing are disruptive in a similar way, as they sap people's time and attention and interrupt their activities" (Solove, 2006). To elicit requirements for information invasions, below we indicate the use of the QuRUP.

1. Elicitation of Far

   Sam does the elicitation of Far in the QuRUP. To elicit privacy requirements which regulate privacy invasion harms, we analyse a special case in which a data holder repeatedly requests data subjects to obtain their personal information. In this invasive case, frequent and repeated requests from the data holder interrupts the activities of data subjects. From this scenario, we assume that *Sam* might construct the following Far which indicates an information invasion scenario.

   Far Query-Repeatedly. A data holder X repeatedly queries a data subject Y to obtain personal information

   In a computerised system, for example, the data holder might be repeatedly sending emails to data subjects for their personal information. This Far and its actor are modelled in Figure 5.8.

2. Elicitation of Illah underneath Far

   Once more *Sam* does this task. Query-Repeatedly is an input artefact of this task of the QuRUP. We note "interruption of data subjects" is one of the consequences of the accomplishment of Query-Repeatedly. We assume that *Sam* might denote this consequence as an *Illah* underneath Query-Repeatedly. Below we write this *Illah*.

   Illah underneath Query-Repeatedly. Interruption of data subjects

3. Elicitation of Asl

   Maududi narrates that Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) is reported to have said: "if you sought permission three times, and were not granted permission, then you must leave". On the basis of this *Hadith*, *Qas* might elicit the following *Asl* relevant to Query-Repeatedly.

   Asl Knock-Repeatedly. A visitor X repeatedly asks a person Y to allow him to enter the house of Y

4. Elicitation of Hukm for Asl

   From the above mentioned saying and practices of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*), the *Hukm* for Knock-Repeatedly is very clear:

   Hukm for Knock-Repeatedly. No visitor X is allowed to repeat a request to a house owner Y to enter his house

5. Elicitation of Illah underneath Asl

   We assume that *Qas* might elicit protection of one's peace of mind from any interruptions as an *Illah* underneath Knock-Repeatedly. This *Illah* is noted below.

   Illah underneath Knock-Repeatedly. Interruption of a house's owner

   This interruption of a house's owner could possibly cause mental distress to the house's owner.

6. Specify requirement

   Based on a shared *Illah* between Knock-Repeatedly and Query-Repeatedly identified

above, the *Hukm* of Knock-Repeatedly can be extended to specify *Hukm* for Query-Repeatedly. From the *Hukm* of Query-Repeatedly, *Qas* might conclude the following privacy requirement.

Requirement for Query-Repeatedly. No person X is allowed to repeatedly query a data subject Y to obtain personal information

Privacy requirements elicited above by using QuRUP on the PIdM correspond to various Ahkamic values. In Section 5.5, we indicate which requirement correspond to which Ahkamic value. From the requirements elicited above, other requirements can also be elicited. On the basis of the requirements elicited above, we tentatively conclude that a "cyber private sphere" constituted by these nine privacy requirements can be considered as an extension of the DoCoMo. These elicited privacy requirements are harmonious with the *Ahkam* constituting the DoCoMo. We note that in the cyber private sphere of the PIdM, privacy requirements fall on data subjects, data holders, and other people. However, Quranic privacy requirements also apply to a state or government whether or not they are operating technological systems. On the basis of the Quranic verse 49:12, Maududi concludes that it is not allowed for an Islamic state to monitor people's private affairs. According to Hayat, an Islamic government is not allowed to infringe on one's private sphere of life (Hayat, 2007).

5.5 Summary of requirements

In Table 2, we summarise the requirements that are elicited using the QuRUP. In this table, we name each requirement as its corresponding Far from which this requirement is elicited. Requirements presented in this table correspond to various Ahkamic values. For example, requirement Collect-pubInfo corresponds to permitted values of *Mubah*. Requirement Insecure-Info corresponds to the obligatory value of *Waajib*. All other elicited requirements correspond to *Haraam* and are prohibitions. In this analysis, we did not come across any *Mandub* or *Makruh* requirement. Ahkamic values which correspond to each requirement are indicated in the forth column of Table 2.The foregoing analysis of the PIdM identifies requirements on data subjects, data holders, and other people for protecting individual's privacy. The third column of Table 2 specifies the actor or actors responsible

Table 2: *A summarised form of privacy requirements in the PIdM*

Requirement	Requirement description	Responsible actor	Hukm
Collect-Info	An unauthorised data collection	data holders	*Haraam*
Collect-Surveillance	Data collection by surveillance	data holders	*Haraam*
Collect-Extort	Data collection by extortion	data holders	*Haraam*
Collect-Pry	Data collection by prying	data holders	*Haraam*
Collect-noSalaam	Data collection without Salaam	data holders	*Haraam*
Collect-pubInfo	Collection of publicly available data	data holders	*Mubah*
Insecure-Info	To secure one's own and others' personal data	everyone	*Waajib*
Reveal-Info	To disclose one's own and others' personal data	everyone	*Haraam*
Query-Repeatedly	Repeatedly demanding other people's personal data	data holders	*Haraam*

for the performance or the non-performance of requirements. From this column one can clearly see that which requirement falls on data subjects which requirement falls on data holders, and which requirement falls on everyone (data holders, data subjects, and other people).

5.6 Summary

Solove (2006) categorises privacy-related invasions into four groups. For software systems, these four groups are information collection, information processing, information dissemination, and information invasions. These four groups of activities can have multiple subgroups. We indicate how the QuRUP can be applied to elicit these subgroups of activities. By indicating an application of the QuRUP on the PIdM, we elicited requirements which correspond to four main groups of privacy-related activities. We show elicited requirements in Table 2. In this table, Collect-Info, collect-Surveillance, Collect-Extort, Collect-Pry, Collect-noSalaam, and Collect-pubInfo are related to information collection group. Insecure-Info is an information processing requirement. Reveal-Info and Query-Repeatedly correspond to information dissemination and information invasion groups respectively.

CHAPTER 6

Evaluation

Contemplating deeply for one hour (with sincerity) is better than 70 years of mechanical worship (Prophet Muhammad)

In order to respond appropriately to the Quranic concerns of Muslim system stakeholders, we customise the RUP to the QuRUP. The Quranic concerns denote fears and desires of Muslims. Their fears are their involvement in a system activity that is against the injunction of the Quran, and their desires concern their involvement in a system activity that is harmonious with the injunctions of the Quran.

As indicated before in Section 1.2, we argue that the QuRUP enables its practitioners to appropriately respond to the concerns of Muslim system stakeholders. Our argument has three steps. We first argue that an appropriate response to any situation has two important and necessary characteristics: that the response is due, *i. e.*. relevant; and that the response is diligent, *i. e.*. carefully performed. The second and third steps of our argument are to evaluate the dueness and the diligence of the QuRUP, in comparison to the RUP, for a situation requiring requirements elicitation from Muslim system stakeholders.

We evaluate the dueness of the QuRUP for its relevance to *Qiyas* and by assessing the quality of the artefact it produces, *i. e.* requirements. *Qiyas* is an appropriate way to consult the Quran to seek its guidance. Therefore, we choose *Qiyas* to evaluate the dueness of the

QuRUP.

The other part of the evaluation criteria involves the attainment of high quality requirements. In this thesis, we assess the output artefact of the QuRUP for five quality attributes of requirements: completeness, consistency, correctness, prioritisation, and traceability. These attributes are considered important for the success of a system with requirements. We choose to assess requirements for quality attributes because we think that a duly diligent RE process would entail high quality requirements. We evaluate dueness of the QuRUP by comparing it with the RUP. To evaluate the QuRUP for attainment of high quality requirements, we use the requirements elicited through it.

Before evaluating the QuRUP on the basis of elicited requirements for the PIdM, we perform a preliminary analysis on the elicited requirements. We perform this preliminary analysis on elicited requirements so that requirements be effectively evaluated. In Section 6.1 of this chapter, we analyse the requirements elicited by applying the QuRUP on the PIdM. Subsequent to requirements analysis, in Section 6.2, we evaluate the QuRUP for dueness by examining its relevance to *Qiyas*. In Section 6.2, we evaluate the QuRUP for dueness by examining the requirements for ascertaining their quality.

6.1 Requirements analysis

In requirements analysis, we eliminate superfluous requirements and generate sophisticated ones. In analysing the requirements of the PIdM elicited through the QuRUP, in Section 6.1.1 we examine requirements of the PIdM presented in Table 3 to remove any redundant requirements. In Section 6.1.2 we generate sophisticated requirements. For the convenience of the readers of this thesis, we replicate requirements in Table 3 from Table 2 presented in a previous chapter.

Table 3: *A summarised form of privacy requirements in the PIdM*

Requirement	Requirement description	Responsible actor	Hukm
Collect-Info	an unauthorised data collection	data holders	*Haraam*
Collect-Surveillance	data collection by surveillance	data holders	*Haraam*
Collect-Extort	data collection by extortion	data holders	*Haraam*
Collect-Pry	data collection by prying	data holders	*Haraam*
Collect-noSalaam	data collection without Salaam	data holders	*Haraam*
Collect-pubInfo	collection of publicly available data	data holders	*Mubah*
Insecure-Info	to secure one's own and others' personal data	everyone	*Waajib*
Reveal-Info	to disclose one's own and others' personal data	everyone	*Haraam*
Query-Repeatedly	repeatedly demanding other people's personal data	data holders	*Haraam*

Table 4: *A summarised form of non-redundant requirements in the PIdM*

Requirement	Requirement description	Responsibility	Hukm
Collect-Info	an unauthorised data collection	data holders	*Haraam*
Collect-pubInfo	collection of publicly available data	data holders	*Mubah*
Insecure-Info	to secure one's own and others' personal data	everyone	*Waajib*
Reveal-Info	to disclose one's own and others' personal data	everyone	*Haraam*
Query-Repeatedly	repeatedly demanding other people's personal data	data holders	*Haraam*

6.1.1 Elimination of superfluous requirements

Requirements can be redundant; that is, one requirement can be contained in another requirement. We examine the requirements of the PIdM to remove such redundancy. Removing redundancy from the requirements obviates any unnecessary analysis in the evaluation of the QuRUP. We note that Collect-Surveillance, Collect-Extort, Collect-Pry, Collect-noSalaam are subsumed under the privacy requirement Collect-Info. Requirements Collect-Surveillance, Collect-Extort, and Collect-Pry specify the scenario of data collection without permission. This scenario, in addition to other scenarios, is addressed in Collect-Info. The requirement Collect-noSalaam specifies a scenario of data collection without offering *Salaam* to data subjects. This scenario is also addressed in Collect-Info.

We find no other redundant requirement in the list of requirements of the PIdM. After elimination of superfluous requirements, we present requirements of the PIdM in Table 4.

6.1.2 Detailed requirements

From the elicited requirements, we generate some sophisticated requirements. To discover these requirements, we analyse non-redundant requirements of the PIdM. These non-redundant requirements are shown in Table 4.

6.1.2.1 Detailed requirements from Collect-Info

The first requirement Collect-Info under analysis is "No data holder X is allowed to collect personal information of any data subject Y without saying *Salaam* to Y and obtaining approval of Y". This requirement is derived from the Quranic verse 24:27. In explaining this verse of the Quran, Maududi mentions that in the *Shariah*, the correct method of seeking approval is to disclose one's identity first and then ask for permission. Maududi narrates the practice of Umar, a companion of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*), of seeking approval and offering *Salaam* to the inhabitants of a house. Maududi mentions that Umar when visiting Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) used to say "Assalam-o- alaikum ya Rasul-Allah [peace be upon you O Phophet of God], I am Umar: May I enter". This narration of Maududi indicates three important things. The first is that for seeking approval, one must reveal his identity and then ask for permission. The second important thing is the sequence in which requirements need to be fulfilled to enter someone else's house. The third important thing is that the visitor must not enter someone's house until permission is granted. Based on this analysis which essentially explains in detail the requirement Collect-Info, we generate the following six requirements. We consider these six requirements as advanced requirements of Collect-Info.

1. Requirement for offering Salaam

   Offering *Salaam* is a requirement before any data collection from data subjects. We state this requirement as below.

   Offer-Salaam. Without offering *Salaam*, no data holder X is allowed to collect any personal information of a data subject Y

2. Requirement for revealing identity

   This requirement states that data holders must reveal their identities before collecting any personal information of data subjects. We state this requirement as below.

Reveal-Id. Without revealing identity, no data holder X is allowed to collect personal information of a data subject Y

3. Requirement for offering Salaam before revealing identity

   Maududi's explanation of the procedure for entering other people's houses indicates that the visitor needs to offer *Salaam* before revealing his identity. However, we do not find any explicit *Hukm* that states this. However, the practice of Calif Umar shows that offering *Salaam* proceeds the revealing of identity. Calif Umar exercised this practice in the presence of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*), and the Prophet did not object this practice. In the *Shariah*, any act which is performed in the presence of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) and to which he did not object is considered as *Mandub*. Therefore, we classify the act of offering *Salaam* before revealing identity as a *Mandub*. We state it as a requirement which is listed below.

   Salaam-Id. It is recommended that every data holder X must offer *Salaam* to a data subject Y before revealing his/her identity to Y [Or].

   Salaam-Id. It is recommended that every data holder X must perform Offer-Salaam before Reveal-Id.

4. Requirement for seeking permission

   This requirement specifies a necessary condition on data holders to seek permission from data subjects before collecting their personal information. We state this requirement as below.

   Request-permission. Without seeking permission, no data holder X is allowed to collect personal information of a data subject Y

5. Requirement for revealing identity before permission

   From Umar's practice of entering the house of Prophet Muhammad (*Sallallahu Alaihi wa Sallam*), we note that he revealed his identity before requesting to enter the house. We consider it a *Mandub* to reveal one's identity prior to seeking permission. For the PIdM, we generate the following related requirement.

Table 5: *A summarised form of detailed privacy requirements of the PIdM*

No.	Requirement	Requirement description	Responsibility	Hukm
1	Offer-Salaam	to offer Salaam before data collection	data holders	*Haraam*
2	Reveal-Id	to disclose identity before data collection	data holders	*Haraam*
3	Salaam-Id	to offer Salaam before disclosing identity	data holders	*Mandub*
4	Request-permission	to request permission for data collection	data holders	*Haraam*
5	Id-permission	to reveal identity before request for permission	data holders	*Mandub*
6	Consent-permission	before collection obtain the consent of data subject	data holders	*Haraam*
7	Collect-pubInfo	collection of publicly available data	data holders	*Mubah*
8	Secure-otherInfo	to secure others people's personal data	data holders	*Waajib*
9	Secure-ownInfo	to secure one's own personal data	everyone	*Waajib*
10	Reveal-Info	to disclose others' personal data	data holders	*Haraam*
11	Query-Repeatedly	repeatedly demanding other people's personal data	data holders	*Haraam*

Id-permission. It is recommended that every data holder X must reveal his identity to a data subject Y before requesting permission from Y

6. Requirement for obtaining consent before collection

   The requirement Collect-Info specifies that it is prohibited to collect other people's personal information without prior approval from them. We specify this part of the privacy requirement as below.

   Consent-permission. Without obtaining permission, no data holder X is allowed to collect personal information of a data subject Y

We present these advances requirements in Table 5. In this table, we also show the responsible actor for the performance or the non-performance of each requirement.

6.1.2.2 Detailed requirements from Query-Repeatedly

We do not find other requirements arising from Query-Repeatedly. However, we note that some details about this requirement. Maududi narrates that Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) is reported to have enjoined that permission should be asked thrice at the most. If there is no reply even at the third call, one should come back. Based on this *Hadith*, we quantify "repeatedly query" in the requirement "No person X is allowed to repeatedly query to a data subject Y for obtaining personal information" to three

times. We also do not find any advanced requirement arising from Collect-pubInfo and Reveal-Info.

6.1.2.3 Detailed requirements from Insecure-Info

This requirement comes from the Quranic verses 24:30-31. In these verses, believers are commanded to restrain their gazes and protect their private parts. An *Illah* underneath "restrain their gazes" is protection of other people's privacy. An *Illah* underneath "protect their private parts" is protection of one's own privacy. From these verses, we conclude that not only the protection of other people's privacy is *Waajib*, but protection of one's own privacy is also *Waajib*. We name Secure-otherInfo and Secure-ownInfo as two requirements corresponding to these two *Waajib*. We state these two requirements as below.

Secure-otherInfo. Every data holder X must secure personal information of a data subject Y

Secure-ownInfo. Every data subject Y must secure his own personal information.

In the following section, we use the requirements presented in Table 5 to evaluate the QuRUP. We evaluate the QuRUP by comparing it with the RUP. For this evaluation we assume that in a RUP-based analysis of the PIdM, the system analyst is non-Muslim, and he does not seek any guidance from the Quran in the performance of the requirements elicitation task. We also assume that the system analyst is aware of Solove (2006), and he uses requirements categorisations of Solove (2006) in his analysis of the PIdM.

6.2 Evaluation of the QuRUP for dueness

We evaluate the QuRUP for dueness by examining its relevance to *Qiyas* and by examining the attainment of high quality requirements. In Section 6.2.2, we provide our evaluation of the QuRUP for its attainment of quality attributes of requirements. The other check to evaluate the QuRUP is to examine its relevance to *Qiyas*. In Section 6.2.1, we provide this evaluation.

6.2.1 Relevance to Qiyas

First we evaluate the QuRUP for dueness by examining the relevance of the QuRUP to *Qiyas*. To examine the QuRUP for its relevance to *Qiyas*, we compare the structure of the QuRUP with the structure of *Qiyas*. We argued that for an appropriate Quranic requirements

Table 6: *Relevance of the QuRUP with Qiyas*

No.	Tasks in *Qiyas*	Tasks in QuRUP	Tasks in the RUP
1	identification of *Far*	Yes	Yes
2	identification of *Asl*	Yes	No
3	identification of *Illah*	Yes	No
4	identification of Hukm of *Asl*	Yes	No

elicitation process, it must contain the structure of *Qiyas* or a structure equivalent to it.

The structure of *Qiyas* is the list and sequence of tasks, roles specified to accomplish these tasks, and methods to accomplish these tasks. In other words, for a process to be duly diligent to address the Quranic concerns, it must contain all tasks of *Qiyas*, roles to accomplish these tasks, and method of *Qiyas* for accomplishing these tasks.

In Table 6, we present a summary of the examination of the QuRUP for its relevance to *Qiyas*. In this table, we also provide the summary of our assessment of the RUP for its relevance to *Qiyas*. In column 2 of this table we list tasks of *Qiyas*. Column 1 is the sequence in which tasks of *Qiyas* are performed. In column 3, we indicate whether or not a task or tasks in the QuRUP serve the purpose of any corresponding tasks in *Qiyas*. In column 4, we indicate whether or not a task or tasks in the RUP serve the purpose of any corresponding tasks in *Qiyas*.

We observe that for every task of *Qiyas*, there is an equivalent task or tasks in the QuRUP. However, we do not find tasks in the RUP equivalent to every task of *Qiyas*. Task 5 and Task 6 (identification of *Asl* and *Hukm* of *Asl*) in the QuRUP equate to Task 2 in *Qiyas*. Task 3 (identification of *Far*) in the QuRUP is equivalent to Task 1 in *Qiyas*. Task 4 and Task 7 (identification of *Ilal* underneath *Far* and *Asl* respectively) in the QuRUP are equivalent to Task 3 in *Qiyas*. Task 8 in the QuRUP serves the purpose of Task 4 in *Qiyas*. We think that the combination of two tasks of the RUP— "gather information" and "conduct requirements worshops" — roughly equate to Task 1 of *Qiyas*. We do not find any task in the RUP which may be equivalent to Tasks 2-4 of *Qiyas*.

We assume that tasks of the QuRUP which are equivalent to the tasks of *Qiyas* are also performed with the same dueness and diligence as they are performed in *Qiyas*. Based on the comparisons depicted in Table 6, we conclude that the QuRUP is relevant to *Qiyas*, but the RUP is not quite relevant to *Qiyas*. In other words, the QuRUP enables its practitioners

to accomplish Quranic due diligence.

As stated before, a duly diligent RE process would entail high quality requirements. In Section 6.2.2, we evaluate the QuRUP for attainment of high quality requirements. Beside evaluating the QuRUP, in this section we indicate how practitioners of the QuRUP would apply it to attain these quality-attributes.

6.2.2 Attainment of high quality requirements

In this section, we evaluate our argument that a duly diligent application of the QuRUP would entail high quality requirements. We examine the quality of requirements based on the attributes of completeness, consistency, correctness, prioritisation, and traceability. Completeness, consistency, correctness, prioritisation, and traceability are quality attributes of software requirements. We evaluate the QuRUP for attainment of these five attributes.

To evaluate the QuRUP for the requirement of traceability, we indicate how requirements elicited through the QuRUP could be traced back to their source. To evaluate the QuRUP for the requirement of prioritisation, we indicate how Quranic requirements are prioritised in the QuRUP. We also compare the process of requirements prioritisation in the QuRUP and in the RUP. To evaluate the QuRUP for requirements consistency, we evaluate the requirements elicited through the QuRUP for their consistency with relevant Quranic *Ahkam*. To evaluate the QuRUP for requirements correctness, we use an Ahkamic diagram to communicate requirements to Muslim stakeholders. The Ahkamic diagram is a useful tool to communicate requirements to system stakeholders. Our evaluation for the correctness of elicited requirement is by inspection by a Quranic expert. To evaluate the QuRUP for requirements completeness, we compare the QuRUP with the RUP to identify requirements which might have remained uncovered by any of these processes.

Below we discuss how each quality attribute can be attained in the QuRUP. We also discuss how the attainment of these quality attributes in the QuRUP differs from the attainment of these quality attributes in the RUP.

6.2.3 Requirements completeness

By applying the QuRUP on the PIdM, various requirements are elicited. We present a summarised form of these requirements in Table 5. These requirements are very revealing.

Table 7: *An evaluation of the QuRUP for requirements completeness*

No.	Requirement	Elicitation by RUP?	Elicitation/non-Elicitation reason
1	Offer-Salaam	No	relevance to the Quranic Ahkam
2	Reveal-Id	Yes	relevance to Solove's taxonomy
3	Salaam-Id	No	relevance to the Quranic Ahkam
4	Request-permission	Yes	relevance to Solove's taxonomy
5	Id-permission	No	relevance to Solove's taxonomy
6	Consent-permission	Yes	relevance to the Quranic Ahkam
7	Collect-pubInfo	Yes	relevance to Solove's taxonomy
8	Secure-otherInfo	Yes	relevance to Solove's taxonomy
9	Secure-ownInfo	No	relevance to the Quranic Ahkam
10	Reveal-Info	Yes	relevance to Solove's taxonomy
11	Query-Repeatedly	Yes	relevance to Solove's taxonomy

We note that among these elicited requirements, there are some requirements that in our opinion are likely to be missed in an RUP-based analysis unless its practitioners put special effort in requirements elicitation of Muslims.

Our evaluation of the QuRUP from the perspective of requirements completeness is summarised in Table 7. In this table, requirements that in our opinion can be elicited by the RUP are marked by Yes, and the requirements that we think are likely to be missed by using the RUP are indicated by No. In the fourth column of Table 7, we give the reason for thinking a certain requirement is likely to missed or otherwise by a RUP-based analysis. We think that requirement 1, requirement 3, requirement 5, and requirement 9 are the requirements likely to be missed by using the RUP for requirements elicitation. However, requirement 2, requirement 4, requirement 6, requirement 7, requirement 8, requirement 10, and requirement 11 can be elicited by applying the RUP alone. We remind the readers that all these requirements are elicited by using the QuRUP.

In the case of requirement 1 and requirement 3, there is an explicit requirement of offering *Salaam* to the person who wants to collect other people's private information. In the analysis of the PIdM, the requirement of offering *Salaam* to data subjects before data collection from them is an important and mandatory requirement for Muslim stakeholders. In other words, it is not allowed to collect people's personal information without offering them *Salaam*. We note that the requirement of offering *Salaam* can be identified only from the Quran or from the secondary sources of the *Shariah*. We are unaware of any other

non-Islamic source, including Solove (2006), for deriving this requirement. In the RUP, we do not find the Quran as a source of requirement or any activity specified for eliciting requirements from the Quran. Therefore, without any support from the Quran in a RUP-based analysis, the requirement of offering *Salaam* is highly likely to be undiscovered.

We think that it is unlikely that a RUP-based analysis would elicit requirements 5 and 9. According to requirement 5, it is recommended that data holders reveal their identity to data subjects before seeking their permission for data collection. We do not find any requirement relevant to requirement 5 in Solove (2006). It implies that in any analysis, including a RUP-based analysis, even when performed by an analyst who is aware of Solove (2006), it is unlikely to discover requirement 5. Requirement 9 is an obligation for everyone to secure their personal information. We do not find any requirement relevant to requirement 9 in Solove (2006). It implies that in any analysis, including a RUP-based analysis, performed by an analyst who is aware of Solove (2006), it is unlikely to discover requirement 9.

We think that a system analyst who has an understanding of Solove (2006) would elicit requirements 2, 4, 6, 7, 8, 10, and 11 in a RUP-based requirements elicitation. For example in case of requirements 8, people's personal information is protected from any disclosure by data holders. In the RUP, this requirement is likely to be elicited as a confidentiality requirement. Similarly in case of requirements 2, 4, 6, 7, 10, and 11, a RUP-based analysis would likely uncover them because the essence for all these requirements is well known in the area of security and privacy. For instance, this essence is known to Solove and it is also discussed in Solove (2006). In short for the elicitation of requirements 2, 4, 6, 7, 8, 10, and 11, there is no need to understand the Quran or any other legal text. For generating these requirements using the RUP, the system analyst only needs technical knowledge about privacy invasions. Interviews with system users and other stakeholders can also be handy for eliciting these requirements.

6.2.4 Requirements prioritisation

In the *Shariah*, all *Ahkam* are not of equal value; that is, some *Ahkam* have priority over the other *Ahkam*. For example, preventing harm takes priority over securing a benefit. Public interest has priority over private interest. The definitive *Qatai* has priority over the probable, *Dhanni*. A definitive *Hukm* or requirement is that which is a direct *Hukm* in

Table 8: *Prioritised privacy requirements of the PIdM*

Priority	Requirement	Requirement description	Responsibility	Hukm
1	Offer-Salaam	to offer Salaam before data collection	data holders	*Haraam*
1	Reveal-Id	to disclose identity before data collection	data holders	*Haraam*
1	Request-permission	to request permission for data collection	data holders	*Haraam*
1	Consent-permission	before collection obtain the consent of data subject	data holders	*Haraam*
1	Reveal-Info	to disclose others' personal data	data holders	*Haraam*
1	Query-Repeatedly	repeatedly demanding other people's personal data	data holders	*Haraam*
2	Secure-otherInfo	to secure others people's personal data	data holders	*Waajib*
2	Secure-ownInfo	to secure one's own personal data	everyone	*Waajib*
3	Salaam-Id	to offer *Salaam* before disclosing identity	data holders	*Mandub*
3	Id-permission	to reveal identity before request for permission	data holders	*Mandub*
4	Collect-pubInfo	collection of publicly available data	data holders	*Mubah*

the Quran or *Sunnah*. Probable *Hukm* or requirements are that which is derived from a definitive or probable *Hukm*. All *Ahkam* or requirements derived via *Qiyas* are probable. Rights of *Allah* have priority over rights of the humans. Prevention of *Haraam* has priority over the attainment of *Halal*.

In Table 5, we do not have any requirement which is definitive or specifies rights of *Allah*. All requirements in this table are probable. Therefore, we therefore, prioritise requirements on the basis of the criterion "prevention of *Haraam* has priority over the attainment of *Halal*". We prioritise the requirements of Table 5 into Table 8. In Table 8, all requirements which have *Haraam* as their *Hukm* have higher standing in the priority. Within other requirements, *Waajib* requirements have high priority as compared with *Mandub* or *Mubah* requirements. Similarly, *Mandub* or recommended requirements have higher priority than *Mubah* or free-choice requirements.

In Table 5, there is no requirement with *Hukm Makruh*. Had there been any *Makruh*, by analogy with in the prioritisation criteria, this would have been placed up in priority to Mandub and Mubah.

6.2.5 Requirements correctness

The QuRUP provides a structure to derive Quranic requirements for software systems. The correctness of software requirements depends on the correct application of the elicitation process and the correctness of elicited requirements. Elicited requirements which are free from errors are correct requirements. In the QuRUP, all elicited requirements are harmonised with the Quranic *Ahkam* through *Qiyas*. According to the *Shariah*, only a Quranic expert can reliably perform *Qiyas* and determine the correctness of a requirement derived from the Quran.

To determine the correctness of our use of *Qiyas* in the QuRUP, we seek review from Shaikh Rafat Najm of the QuRUP. Shaikh Rafat Najm is an *Imam* at the Auckland University of Technology *Masjid*. We also seek his review on the correctness of elicited requirements and their appropriateness to the Quranic *Ahkam*. He hailed our correct use of *Qiyas* in the QuRUP. He also appreciated the elicitation of *Salaam*-related requirements for software systems. However, he has shown concerns for appropriateness of *Asl* in requirements 8 and 9. However, he did not reject the appropriateness of *Asl*, but he described these requirements as controversial. According to him, the relevance of *Asl* in requirements 8 and 9 might be appropriate to one Quranic expert and inappropriate to another.

6.2.6 Requirements traceability

The practitioners of a duly diligent process need to maintain the necessary documentation related to the process. Maintaining the documentation is helpful for a due diligence defence. From this documentation, the source of every software requirement can be traced. The QuRUP supports requirements traceability. In the requirements elicited through the QuRUP, every requirement has a related *Far*. Every *Far* has a relevant *Asl*. Every *Asl* is based on a Quranic verse. By following the path from software requirements to Quranic verse, one can construct a traceability link and determine the source of requirements. A Quranic verse which is relevant to a software requirement is the source for this requirement. This link can also be extended to a human source of requirements. Sometimes a *Far* is constructed on the basis of a wish from a system stakeholder. In this case, this stakeholder would be the source of this requirement.

The Quranic verse 24:27 is the source for requirements 1, 2, 3, 4, 5, and 6. The Quranic verse 24:29 is the source for requirement 7. The Quranic verses 24:30-31 is the source for requirements 8 and 9. The Quranic verses 66:3-5 is the source for requirement 10. The source for requirement is 11 an *Hadith* to which Maududi refers in the explanation of the Quranic verse 24:27.

6.2.7 Requirements consistency

We examine consistency between software requirements and Quranic *Ahkam* by mapping the terminologies of software requirements to the terminologies of corresponding Quranic *Ahkam*. The list of criteria that we devise to evaluate the consistency between software requirements and corresponding Quranic requirements includes actor, action, data object, *Illah*, and *Hukm*.

In Table 9, we summarise our evaluation for consistency between requirements. In this table, Column 1 shows the requirement number. Requirements in this table are same as the requirements in Table 5. Column 2, and Column 3, Column 4, Column 5, and Column 6 represent the list of criteria for terminology mapping. We apply this list of criteria to decompose each software requirement and corresponding Quranic requirement into five categories: actor, action, data object, *Hukm*, and *Illah*. In Table 9, for every requirement (1-11) there are two rows against the terminology mapping criteria. For every requirement, row 2 is the terminologies of the software requirement and row 1 is the terminologies of corresponding Quranic requirement.

For example, in requirement 1, there are two actors involved. These two actors are data holder and data subject. In row 1 for this requirement, we show data holder actor only because this requirement conveys *Hukm* on data holders only. In this requirement, *Hukm* is a prohibition or *Haraam* on an action of data holders. In this requirement, information collection without offering *Salaam* is the action of the data holder which is declared *Haraam*. The reason behind this *Hukm* is discomfort of data subjects. In this requirement, data object is personal information of data subjects.

The Quranic verse 24:27 is relevant to privacy requirement 1. In row 1 of requirement 1, we show the terminologies of this verse. In this verse, there are two actors involved: a householder and a visitor. Since the Quranic requirement is on the visitor actor so in Table

Table 9: *An evaluation of the QuRUP for requirements consistency*

No.	Actor	Action	Data object	Illah	Hukm
1	visitor	entrance without offering Salaam	household	discomfort	*Haraam*
	data holder	information collection without offering Salaam	personal information	discomfort	*Haraam*
2	visitor	entrance without revealing identity	household	privacy protection	*Haraam*
	data holder	information collection without revealing identity	personal information	privacy protection	*Haraam*
3	visitor	offer Salaam before revealing identity	household	-	*Mandub*
	data holder	offer Salaam before revealing identity	personal information	-	*Mandub*
4	visitor	enterance without permission	household	privacy protection	*Haraam*
	data holder	information collection without permission	personal information	privacy protection	*Haraam*
5	visitor	reveal identify before requesting permission to enter	household	-	*Mandub*
	data holder	reveal identify before requesting information collection	personal information	-	*Mandub*
6	visitor	enterance in a house without consent	household	privacy protection	*Haraam*
	data holder	information collection without any consent	personal information	privacy protection	*Haraam*
7	visitor	enterance in public houses	public space	choice	*Mubah*
	data holder	collecting publicly available information	public space	choice	*Mubah*
8	individual	control gazes to watch other people	human body	privacy protection	*Waajib*
	data holder	securing other's personal information	personal information	privacy protection	*Waajib*
9	individual	Securing one's own private parts	human body	privacy protection	*Haraam*
	everyone	securing one's own personal information	personal information	privacy protection	*Waajib*
10	individual	Disclosing other's secrets	secrets	privacy protection	*Haraam*
	data holder	disclosing other's personal information	personal information	privacy protection	*Haraam*
11	visitor	repeatedly asking for permission to enter	household	interruption	*Haraam*
	data holder	repeatedly demanding personal information	personal information	interruption	*Haraam*

9, we show only this actor. The *Hukm* being conveyed through this verse is a prohibition or *Haraam*. This prohibition is on an action of a visitor. The *Haraam* action according to this verse is entering other people's houses without offering them *Salaam*. The *Illah* underneath this *Hukm* is discomfort of householder. *Hukm* and *Illah* in both requirements (software requirement and corresponding Quranic requirement) are same.

In requirement 1, data object is people's personal information. In the corresponding Quranic requirement, data object is every kind of private information about people. This includes people's personal information. In both requirements, similar actions are regulated. In both requirements, actors obtain information about an individual without offering *Salaam* to the individual.The notion of actor is also similar in both requirements.

The similarity of the terminologies of requirement 1 to the corresponding Quranic requirement suggests that requirement 1 is consistent with its relevant Quranic requirement.

We decompose other requirements of the PIdM and their corresponding Quranic requirements into five terminologies: actor, action, data object, *Illah*, and *Hukm*. In Table 9, we present a summarised form of the comparison of the terminologies of software requirements elicited for the PIdM and their corresponding Quranic requirements. On the basis of similarity (in terms of actor, action, data object, *Hukm*, and *Illah*) of software requirements and corresponding *Ahkam* presented in Table 9, we conclude that these software requirements are consistent with their corresponding Quranic requirements. We could not find *Illah* for requirements 3 and 5.

Based on our evaluation of the QuRUP, we find no evidence that the QuRUP is not a duly diligent process for addressing the Quranic concerns. A process is duly diligent if its structure enables its practitioners to achieve dueness and diligence. However, we find evidence that the RUP is not a duly diligent process for addressing the Quranic concerns of Muslim system stakeholders. Our criteria for evaluation of dueness in the QuRUP are its relevance to *Qiyas* and attainment of quality attributes of requirement.

In evaluating the QuRUP for its relevance to *Qiyas*, we find that *Qiyas* is contained in the QuRUP. Every task of *Qiyas* is present in the QuRUP. Roles specified for tasks in *Qiyas* are the same as those specified for the respective tasks in the QuRUP. This indicates that the QuRUP is an appropriate process to derive requirements from the Quran (*Qiyas* is an appropriate tool which Islamic jurists use to consult the Quran). The correct performance of *Qiyas*-related tasks in the QuRUP depends on the diligence of people who accomplish these tasks.

In evaluating the QuRUP for attainment of quality attributes, we assess five important quality attributes of requirements: completeness, consistency, correctness, prioritisation, and traceability. For evaluating requirements completeness, we indicate some important requirements that might not be elicited by an unmodified RUP. However, these important requirements are elicited by the modified RUP, the QuRUP. For instance, requirements 1, 3, 5, and 9 were elicited in a case study of the PIdM. These requirement might have remained undiscovered in a RUP-based analysis.

Requirements prioritisation in the QuRUP differs from the requirements prioritisation in the RUP. In the RUP, requirements engineers prioritise requirements often on the basis

of system users' feedback. In the QuRUP, however, requirements prioritisation rests on the basis of the criteria provided in the *Shariah*. These criteria cannot be overridden by end users' feedback. However, within a certain category, requirements can be prioritised on the basis of the feedback from system end users. For example, if there are multiple requirements which have the *Hukm Haraam*, then these requirements can be prioritised with each other on the basis of the feedback from end users. However, all these requirements whose *Hukm* is *Haraam* will remain a higher priority than all other types of requirements.

We do not find any major difference between the QuRUP and the RUP, in principle, in the evaluation of requirements for their consistency, tractability, and correctness. To communicate requirements to end users, we extend the use-case paradigm to an Ahkamic diagram so that requirements could be effectively communicated to Muslim stakeholders.

A retrospective look on the evaluation of the QuRUP reveals that requirements prioritisation in the QuRUP is significantly different from requirements prioritisation in the RUP. The QuRUP enables its practitioners to elicit more important requirements of Muslim stakeholders than requirements elicited through the RUP. The QuRUP and the RUP are in principle not different in their attainment of requirements correctness, consistency, and traceability.

Our analysis of the PIdM has two limitations: first, that we did not elicit all possible *Asl* from the Quran, and second that, we did not elicit requirements from each and every possible variation of each elicited *Asl*. For example, there are some special conditions which may allow intrusions into one's house. Likewise, there are exceptional conditions in which one is allowed to disclose other people's personal information to a third party. In order to keep our analysis simple, we do not apply QuRUP to these exceptional cases. In future work, we plan to extend our research to encounter all possible Quranic *Asl*, including exceptional cases, for a software system.

Another weakness of the analysis is the attainment of a limited set of quality attributes. In the evaluation of the QuRUP, we considered only five attributes as important ones, but there could be other quality attributes attainable by the QuRUP. For instance, unambiguity is also an important attribute for requirements. A careful examination of the requirement Query-Repeatedly reveals that this requirement is ambiguous. This requirement specifies that data holders are allowed to ask for people's personal data not more than three times

during a session. This requirement does not articulate the length of the session. A developer may think that the session could be a second, minute, an hour, or a day. This requirement can be made unambiguous by declaring the session length. The Quran does not restrict us in the specification of session time. So the practitioners of QuRUP may freely set a session length for Query-Repeatedly requirement. They can specify the session length according to the nature of system. Due to the Quranic freedom, session length can vary from one system to another. This resolution of ambiguity in the requirement Query-Repeatedly is indicative only. Thus, other requirements could also be analysed for ambiguity and other attributes.

6.3 Summary

An appropriate response to a situation has two characteristics: dueness and diligence. The dueness in requirements elicitation of Muslim stakeholders is the relevance of RE process to *Qiyas*. *Qiyas* is an appropriate method to consult the Quran. The diligence in requirements elicitation of Muslim stakeholders is the carefulness of the practitioners in applying the QuRUP. A duly diligent application of a RE is likely to entail high quality requirements. Among others, completeness, correctness, consistency, prioritisation, and traceability are important quality attributes of requirements. The QuRUP contains the structure *Qiyas*, and its diligent application produces important high quality requirements. By applying the QuRUP, its practitioners can establish due diligence in the development of a software system which has Muslims as its important stakeholders.

CHAPTER 7

Conclusion

To listen to the words of the learned and to instill into others the lessons of science is better than religious exercises (Prophet Muhammad)

In software engineering, stakeholder satisfaction is vital; an appropriate response to the Quranic concerns of Muslim system stakeholders has remained relatively unexplored. To appropriately respond to the concerns of Muslim system stakeholders, we develop the QuRUP.

The QuRUP is a duly diligent RE process. We earmark this process for Quranic requirements elicitation with due diligence. For eliciting the Quranic concerns of Muslim system stakeholders, we apply the QuRUP to a software system. In eliciting Quranic requirements by using the QuRUP, we identify relevant *Ahkam* from the Quran. The Quran contains general *Ahkam* which regulate a societal system. These *Ahkam* specify requirements on human actions and inactions. As long as Muslims fear *Allah*, they must obey all these *Ahkam*.

In Chapter 3, we review Quranic *Ahkam* on individual's privacy and synthesise these *Ahkam* into three types. These three types constitute DoCoMo. DoCoMo consists of domestic, communication, and modesty related *Ahkam*. By using the QuRUP, we extend these *Ahkam* to model privacy requirements for software system with privacy concerns. We use

these requirements to evaluate the QuRUP.

We evaluate the QuRUP for its relevance to *Qiyas* and attainment of high quality requirements. In the *Shariah*, *Qiyas* is an appropriate way to consult the Quran for matters not explicitly regulated in the *Shariah*. The other check to evaluate the QuRUP is the attainment of high quality requirements. We assess the quality of requirements for five important attributes: completeness, correctness, conciseness, traceability, and prioritisation.

In evaluating the QuRUP, we find that it contains tasks equivalent to the tasks of *Qiyas*. We also find that requirements elicited by using the QuRUP satisfy the five quality attributes criteria. By finding the relevance of the QuRUP to *Qiyas* and the attainment of high quality requirements, we conclude that the QuRUP is a duly diligent RE process. The QuRUP is duly diligent because it meets our argued characteristics (dueness and diligence) of an appropriate response to a situation. The QuRUP is duly diligent for a situation which requires an appropriate response to the concerns of Muslim system stakeholders. The dueness in the QuRUP is its relevance to *Qiyas* and attainment of high quality attributes. The diligence in the QuRUP is the carefulness of its practitioners in applying the QuRUP.

Our evaluation of the QuRUP is in comparison with the RUP. In examining the relevance of the RUP to *Qiyas*, we find that the RUP is not relevant to *Qiyas*. The RUP is not completely relevant to *Qiyas* because it covers only one task of *Qiyas* out of four important and necessary tasks of *Qiyas*. Since the RUP does not contains all tasks of *Qiyas*, the RUP is not an appropriate way to consult the Quran.

In examining the QuRUP and the RUP for the attainment of high quality requirements, we find provocative results especially in the completeness and prioritisation attributes. We observe that few requirements elicited through the QuRUP were missed by a RUP-based analysis. For example, requirements 1, 3, 5, and 9 are the requirements most likely to be missed by using the RUP for requirements elicitation. These requirements are important for Muslims. The *Hukm* associated with requirement 1 is *Haraam* which is a prohibition. The *Hukm* associated with requirement 9 is *Waajib* which Muslims are required to perform. The *Hukm* associated with requirements 3 and 5 is *Mandub* which is recommended to perform. In Table 7 in Chapter 6, we provide a summary of our assessment of the QuRUP and the RUP for requirements completeness.

For prioritising requirements, the QuRUP is different to the RUP. In the RUP, requirements are prioritised often on the basis of user feedback concerning the importance of requirements. However, in the QuRUP, requirements prioritisation is on the basis of rules of the *Shariah*. The difference between the QuRUP and the RUP for prioritising requirements suggests that the RUP is not appropriate to prioritise Quranic requirements. In Table 8 from Chapter 6, we prioritise requirements in a QuRUP-based analysis. We find no major difference of the QuRUP from the RUP, in principle, for the requirement of consistency, tractability, and correctness.

In order to communicate requirements to system stakeholders, we extend UML use-case diagram to the Ahkamic diagram. We believe that the Ahkamic diagram is an appropriate way to communicate requirements to Muslim system users. However, the Ahkamic diagrams are not an appropriate way to communicate requirements to system developers. To model requirements in a shape from which system developers build a system, Ahkamic diagrams need to be changed to use-case diagrams. In order to transform the Ahkamic diagram to use-case diagram, system engineers will need to separate software requirements from system-wide requirements. Software requirements are then communicated through use-case diagram to system developers.

In this thesis, all elicited requirements by using the QuRUP are essentially extensions of Quranic privacy-related *Ahkam*. For example, requirements 1 through 7, and requirement 11 are extensions of domestic *Ahkam*. Requirements 8 and 9 are extensions of modesty *Ahkam*. Requirement 10 is an extension of communication-related *Ahkam*. By realising that privacy requirements elicited for the PIdM are extensions of Quranic privacy-related *Ahkam*, we conclude the the private sphere in software systems constituted by the privacy requirement is an extension of DoCoMo. The DoCoMo is the private sphere constituted by the Quranic privacy-related *Ahkam*.

Our case study indicates how a QuRUP-based analysis can reveal the Quranic requirements on human actions and inactions when interacting with a software system. Although, to illustrate the proposed process, we analysed one software system, the PIdM, the same process can be applied to other systems. The Quranic privacy requirements conclude some responsibilities of the data subjects (requirement 9) to data holders (requirements 1 through

11), and on others (requirement 9). In addition, we have tentatively identified a permission or *Mubah* (requirement 7). We have seen several types of human responsibilities for privacy. We have not found any guidance, in the Quran, regarding the responsibilities (if any) of inanimate objects such as technological systems. We tentatively conclude that responsibilities always fall on humans, not on our machines or technology.

We beleive that one of reasons behind not having any responsibility of machines is that they can not be capable of doing all that humans can do. Humans are, after all, the best creation in the universe. For security of people's personal information in technological systems, Solove (2006, 2008) give more weight to people than technology. In his privacy taxonomy summarised in Chapter 4, (Solove, 2006) ascribes regulatory bodies as the main source behind privacy invasions in software systems. Solove (2008) indicates that despite taking strong technological measures to protect software systems which contain people's personal information, data holders often readily disclose and/or disseminate data subjects' personal information they have collected. The essence of his argument is that people are the main source, not the technology, behind privacy invasions in software systems which contains personal information. According to him, "the law fails to focus on the causes of information abuses; it has not identified all the responsible parties; and it has not fashioned appropriate remedies to respond to these abuses" (Solove, 2008).

Generally, Quranic privacy requirements apply to system designers, owners, users, and other people interacting with the system. However, Quranic privacy requirements also apply to a state or government whether or not they are operating technological systems. On the basis of the Quranic verse 49:12, Maududi concludes that it is not allowed for an Islamic state to monitor people's private affairs. Hayat (2007) argued that privacy requirements also apply to Islamic states. In his paper reviewed in Chapter 3, on the basis of the story of Umar, Hayat (2007) concluded that Islam respects individual freedom and rights to privacy; it does not allow any Islamic state to invade people's privacy. For software systems, we say that Islamic states are stakeholders of these systems. They are stakeholders because they have a requirement to not invade computer systems which contain private information. The requirement on Islamic states to not violate other's private information also implies that Islamic states are affected by software systems.

We tentatively conclude that a *Muhtasib* (or any other official censor) is not allowed to monitor people's on-line activities on the internet. We conclude this because in our opinion people's internet activities are their private business, and personal information stored on their computers is likewise private. Similarly, we also conclude that an Islamic government is not allowed to install closed-circuit television (CCTV) cameras to monitor people's private activities. CCTV surveillance of private activities violates their right to privacy given to them by *Allah*; therefore, the CCTV surveillance is an *Haraam* act. There is further support for these two conclusions in requirement 1 and requirement 4.

One implication of above drawn conclusions is that an Islamic government, while enshrining the *Amr-bil-Maroof*-wa-*Nahi-anil-Munkar* principle, can deny access to sites that they think are prohibited in the *Shariah*. Defining boundaries for the jurisdiction of *Muhtasib* is an issue particularly when interacting with current day technological systems. Our conclusion, then, is that discovering privacy requirements from the Quran can help specify what is not allowed for a *Muhtasib* to monitor or invade. We hope that our academic arguments, in this thesis, mark the beginning of the end of the period of "remarkable silence" (Cannataci, 2009) regarding *Allah*'s requirements, as revealed in the Quran, on modern technological systems such as identity cards and surveillance devices.

Although our proposal of the QuRUP may seem of concern to only a small group of software engineering community, it should in fact concern anyone who cares about Quranic *Ahkam*. A similar approach can be adopted in other areas such as medicine. In the Islamic world, various initiatives have been taken to enshrine principles of Islam in modern societal and technological systems. For example, to regulate autopsies in Qatar, the government of Qatar enacted a Quranic-compliant law (Bhootra, 2006). The government of Pakistan is in the process of formulating a Quranic-compliant data protection law, and this law would be in harmony with European data protection law (Hayat, 2007)

The proposed process of discovering system privacy requirements is not only useful for Pakistan but for other countries as well. These requirements could help Islamic states to enshrine Quranic principles among Muslims for their interactions with software systems. The basic principles of privacy are, quite possibly, accepted by many different societies with many different religious practices. A better understanding of the Quranic requirements

of privacy will help non-Muslims see similarities and differences between non-QuRUP and the QuRUP-based systems. These requirements could be helpful in understanding Muslims rights and obligations, for those non-Islamic states where a significant number of Muslims are living. Furthermore, any non-Muslim who wants to operate a technological system in the Islamic world, and anyone who wants to provide technological services to Muslims, should be aware of the Quranic privacy requirements. Despite provocative results obtained in this research, this research still have limitations. In the following section, we discuss some limitations of this study and directions to carry out future work.

7.1 Limitations and future work

The research conducted in this thesis is far from definitive; rather this research has provoked some important questions. These questions need to be addressed in order to meet the Quranic concerns of Muslim system stakeholders. Eliciting other types of Quranic requirements in addition to privacy requirements and developing a software system based on these requirements are two prime extensions of our proposal of the QuRUP in responding to concerns of Muslim stakeholders of a software system.

In developing a software system, requirements elicitation is an early-stage activity to understand what is to build. In RUP-based development, use-case diagram is used in early stages of development to capture what is to build or requirements of system stakeholders. In this thesis, we extended the use-case artefact to the Ahkamic diagram.

We extended the use-case diagram to the Ahkamic diagram after realizing that use-case is less helpful in Quranic requirements elicitation and communication. However, the validity of the proposed artifact, *i. e.*, the Ahkamic diagram for its use in "requirements elicitation" and "requirements communication" is a concern. Let us first examine the case of validity of the Ahkamic diagram for its use in requirements elicitation.

We argued in this thesis that use-case diagram is less helpful in eliciting Quranic requirements. We then extended use-case diagram to the Ahkamic diagram and concluded that the Ahkamic diagram is more appropriate than use-case diagram for Quranic requirements elicitation purpose. Our this conclusion has some analytic support in Jorgensen

(2001). Jorgensen (2001) states that use cases cannot accommodate obligations. This implies that the use-case diagram also cannot accommodate obligations or *Waajib*. On the other hand, the Ahkamic diagram can accommodate obligations along with other types of *Ahkam*. Like earlier case, our conclusion about the appropriateness of the Ahkamic diagram can be further strengthened by a formal evaluation of the Ahkamic diagram for its appropriateness over use-case diagram for the purpose of requirements elicitation.

Our case study of the PIdM can be considered as a proof of concept to argue that the Ahkamic diagram is more appropriate than the use-case diagram for requirements elicitation of Muslim system stakeholders. In this case study, was indicated that the process which uses the Ahkamic diagram, *i. e.*, the QuRUP, elicited more important requirements of Muslims than the process which does not use the Ahkamic diagram, *i. e.* RUP. We say that this study is undoubtedly helpful to analyse the potential scope of the Ahkamic diagram, however, we do not believe that this case study is sufficient to conclusively validate our assertion that the Ahkamic diagram is more appropriate than use-case diagram for eliciting requirements of Muslims.

Merely because the QuRUP has, in a particular case, elicited more important requirements than the RUP this difference is not necessarily due to the use of the Ahkamic diagram in the QuRUP. However we did find more important requirements using QuRUP, and QuRUP does use Ahkamic diagrams, so our case study has provided some support for our assertion that the Ahkamic diagram is more appropriate than the use-case diagram for eliciting requirements of Muslims. In future work, we intend to perform a formal evaluation to assess the appropriateness of the Ahkamic diagram over use-case diagram for eliciting requirements of Muslims.

We also made a more sweeping assertion: that the Ahkamic diagram is more appropriate than use-case diagram for requirements elicitation. Note that this statement is not restricted to cases where there are Muslim stakeholders; however for understandability to non-Muslims it would be important to use non-Arabic terms such as “required”, “forbidden”, “encouraged”, “deprecated”, and “optional”. This conclusion has some support from Jorgensen (2001). We encourage others to make a more formal evaluation of the Ahkamic diagram for its appropriateness over the use-case diagram, for the purpose of requirements

elicitation.

This evaluation could be done by eliciting requirements of Muslim as well as requirements of non-Muslim stakeholders of a system by applying the Ahkamic diagram and then use-case diagram and then analysing the output produced. One way to analyse the output is to examine whether or not the Ahkamic diagram was helpful is eliciting more types of important requirements which were overlooked by using use-case diagram alone for requirements elicitation.

A weakness in the forgoing discussion is having an artefact more appropriate than use-case diagram is not adequate to conclude the appropriateness in general of the artefact. Therefore, even if we somewhat conclude that the Ahkamic diagram is appropriate over use-case diagram this would not guarantee that the Ahkamic diagram is the only appropriate tool or that it must be used in requirement elicitation. This opens further avenues of research to compare the Ahkamic diagram with other artefacts which are used to facilitate requirements elicitation.

Now let us go back to examine the case of communicativeness of the Ahkamic diagram. In this thesis, we argued and tentatively concluded that the Ahkamic diagram is communicative to Muslims than use-case diagram. Our conclusion that the Ahkamic diagram is communicative to Muslims rests on the questionable assumption that the Arabic labeling in the Ahkamic diagram lends it communicative to Muslims. This assumption was further strengthened by a personal assessment of the Ahkamic diagrams of this thesis by the author of this thesis who is a non-Arabic speaker Muslim but has familiarity with Arabic language. A further assessment of these diagrams by an Arabic speaker Muslim scholar led us tentatively conclude that the Ahkamic diagram is communicative to Muslims.

Moreover, it is important to consider the possible communicativeness of the Ahkamic diagram to non-Muslims. This can be evaluated by comparing, in an experimental setting, two explanations of a software system with respect to stakeholder understanding and buy-in. The first explanation may consist of some Ahkamic diagrams, with their textual description. The second explanation may consist of some use cases and misuse cases of the same software system. System engineers may “tune” the second explanation, in preliminary experimentation, so that it provides roughly equivalent levels of understanding and

buy-in from non-Muslims as the first explanation. We think that such tuning is possible for non-Muslims (*i. e.*, that Ahkamic diagrams do not impede buy-in and understanding for non-Muslims).

Eliciting other types of Quranic requirements in addition to privacy requirements is another prime extension of our work. In their paper reviewed in Chapter 2, Pfleeger and Pfleeger (2009), while conceding the importance of privacy requirements elicitation, noted that privacy requirements sometimes directly conflict with security requirements. They gave an example to demonstrate the conflict between security and privacy: safeguarding a criminal individual's privacy could jeopardise the security of the public. We agree with (Pfleeger and Pfleeger, 2009) and think that it is not unlikely that stakeholder's requirements of any type elicited through the QuRUP may conflict with each other and with other types of requirements. In saying that systems requirements elicited by using the QuRUP conflict with each other, we are both right and wrong. We are right because we sometimes observe conflicting requirements, for instance the requirements mentioned by (Pfleeger and Pfleeger, 2009). However ultimately we are wrong: Correctly elicited Quranic requirements cannot be in conflict with each other, because the Quran is never in conflict with itself.

On the basis of forgoing discussion, we conclude that requirements which are correctly elicited from the Quran would not be inconsistent or contradictory. Our this conclusion is supported by the fact that Muslims believe that the Quran is free from inconsistencies and contradictions because it is the words of *Allah*, and we can not imagine anything eclipsing *Allah*'s sayings. After asserting that the Quran is the words of *Allah*, we disagree that there would be any inconsistency or contradiction in the Quranic *Ahkam*. Therefore, requirements elicited from the Quran would be consistent and free from any contradictions. We support this argument by indicating a conflict resolution between privacy and security requirements.

Maududi, in explaining the Quranic verse 24:27, mentioned that it is permissible for someone's privacy to be invaded, if otherwise the security of the public would be at risk. This explanation of Maududi is an example of how Quranic guidance can help resolve the conflict between privacy and security identified by Pfleeger and Pfleeger (2009). Maududi's

explanation also indicates the right to privacy is not an inalienable or absolute right. Notwithstanding this conflict resolution, we still do not claim that requirements elicited through the QuRUP would always be consistent and non-conflicting. The QuRUP certainly merits further investigation to see whether or not requirements elicited through the QuRUP are consistent and non-conflicting. We find no contradictory or inconsistent requirements in our analysis of the PIdM.

In addition to conflict between different types of requirements, requirements of different Muslim system stakeholders may conflict with each other. If this conflict is Quranic, then it would be solved by an Islamic scholar or a jurist who are involved in the project. In the case the conflict is not are a religious or Quranic conflict, then it could be resolved by adopting the conflict resolution method of the RUP.

Another type of conflict is between the concerns of Muslims and non-Muslims. Although resolving such conflict is outside the scope of this thesis, we give some general guidelines on how this type of conflict might be resolved.

Conflict between the concerns of Muslims and non-Muslims is considered to be the most critical conflict; it first glance it appears that the QuRUP might fail because of this conflict but a closer inspection of Islamic tradition reveals an appropriate conflict-resolution procedure. The Islamic history informs us that, during and after the life time of Prophet Muhammd (*Sallallahu Alaihi wa Sallam*), non-Muslims were living with Muslims in the Arabic peninsula under the auspices of an Islamic state.

In some historic cases, non-Muslims even willingly agreed to allow some of their social cases to be judged according to the regulation of the Quran. One implication of this history lesson is the Quran has guidances beneficial to both Muslims and non-Muslims. By analogy, then, non-Muslims stakeholders of software system can also take advantage from the teachings of the Quran.

The Quranic teaching is a mercy to not only Muslims but to humanity. We infer this assertion from a verse of the Quran in which *Allah* introduces his Prophet Muhammad (*Sallallahu Alaihi wa Sallam*) as mercy to humanity. The Quran is the message that Prophet Muhammd (*Sallallahu Alaihi wa Sallam*) brought to the humanity. By implication then the Quranic *Ahkam* is mercy to humanity. Asani (2003) has support for our implication.

Asani (2003) while acknowledging the pluralistic vision of Islam asserts that the clash between Muslims and non-Muslims is not as much a clash of civilisations as it is a clash of ignorance. Asani (2003) further refers to the following poetry of Saadi, a Muslim poet, that suggests a conflict-free life.

> Human beings, created from the same essence, are limbs of one another
> When one limb aches, the other limbs are restless, too
> O you who are indifferent to the pains of others
> You do not deserve to be called human

Having argued that the Quran is mercy to humanity and it has teachings to live conflict-free life, let us now turn our attention to those who do not think so. By the way while it is true for Muslims the Quran is mercy to humanity, it does not necessarily follow that everyone should or may believe the Quran is mercy for them. So the question arise if someone does not want to follow the Quran then how can the conflicts of such people be resolved with Muslim system stakeholders.

Resolution of this question is a complicated matter. It is Islamic jurists who have authority to resolve such conflicts. However, in order to resolve issues like this, they may need to understand the nature of conflicts, whether the system under consideration is under the jurisdiction of an Islamic state or not, and who owns the system. If we are right then probably Muslim stakeholders may relinquish their *Mandub*, *Makruh*, and *Mubah* requirements to resolve the conflict. Additionally, if the conflict resolution would engage Muslims in an activity the contravenes the Quran (*i. e.* committing a *Haraam* or leaving a *Waajib* then developing an augmented system or an additional component of the system is probably a solution such that Muslims may not be engaged in activities that contravene the Quran.

We conclude our thesis by saying that the QuRUP is an appropriate response to elicit the Quranic concerns of Muslim system stakeholders. Of course, some readers may disagree with this conclusion that the QuRUP is a duly diligent process. This is perahps because our proposed process and its output is validated by one Islamic scholar, not by an islamic jurist. Even all Islamic scholars do not necessarily think alike, some of them may probably dispute with the validations of Shaikh Rafat. This research is yet to be validated by an

Islamic jurist.

If we accept the authoritativeness of the validation of Shaikh Rafat the QuRUP is a duly diligent process and it will remain so until someone comes up with an improved duly diligent process for addressing the Quranic concerns of Muslim system stakeholders. Last but not least, we seek sincere forgiveness of *Allah* if by mistake we inappropriately interpreted any part of the Quran in this study. *Amin*.

Bibliography

Adrion, W. R., Branstad, M. A., and Cherniavsky, J. C. (1982). Validation, verification, and testing of computer software. *ACM Computing Surveys*, 14:159–192.

Alexander, I. (2002). Initial industrial experience of misuse cases in trade-off analysis. In *Proceedings of the 10th Anniversary IEEE Joint International Conference on Requirements Engineering*, pages 61–70.

Alexander, I. (2003). Misuse cases: use cases with hostile intent. *IEEE Software*, 20(1):58–66.

Alexander, I. (2010). Keynote talk piecing together the requirements jigsaw-puzzle. In Wieringa and Persson (2010), pages 1–1.

Algarni, A. F. (2010). Is a Shari'ah-based law compatible with cybercrime? An inquiry into the Saudi regulations on internet fraud. *Journal of Law, Politics and Societies*, 5(2):1–17.

Allenby, K. and Kelly, T. (2001). Deriving safety requirements using scenarios. In *the 5th IEEE International Symposium on Requirements Engineering (RE'01*, pages 228 –235.

AlSaleh, K. (2009). Interview with CEO of I'mHalal. Available at *http://thenextweb.com/me/2009/11/06/interview-reza-sedaha-ceo-imhalal/*.

Alshech, E. (2004). Do not enter houses other than your own: the evolution of the notion of a private domestic sphere in early Sunni Islamic thought. *Islamic Law and Society*, 11(3):291–332.

Alshech, E. (2007). Out of sight and therefore out of mind: early Sunni Islamic modesty regulations and the creation of spheres of privacy. *Journal of Near Eastern Studies*, 66(4):267–290.

Ambler, S. W., Nalbone, J., and Vizdos, M. J. (2005). *The Enterprise Unified Process: Extending the Rational Unified Process*. Prentice Hall Press, USA.

Amin, L., Sujak, S. F., Samian, A. L., Haron, M. S., Mohamad, M. N., and Othman, M. Y. (2009). Islamic ethics and modern biotechnology. *Sari - International Journal of the Malay World and Civilisation*, 27(2):285–296.

Angwin, D. (2001). Mergers and acquisitions across European borders: national perspectives on preacquisition due diligence and the use of professional advisers. *Journal of World Business*, 36(1):32–57.

Anir, N. A., Nizam, M. N. M. H., and Masliyana, A. (2008). RFID tag for halal food tracking in Malaysia: Users perceptions and opportunities. In *Proceedings of the 7th WSEAS International Conference on Telecommunications and Informatics*, pages 87–92.

Antón, A. I. and Potts, C. (1998). A representational framework for scenarios of system use. *Requirements Engineering*, 3(3/4):219–241.

Aqsha, D. and Begawan, B. S. (2009). Facebook: Is it halal or haram? The Brunei Times, 7 july 2009. Available at *http://www.bt.com.bn/analysis/2009/07/07/*.

Asani, A. S. (2003). So that you may know one another: A Muslim American reflects on pluralism and Islam. *Annals of the American Academy of Political and Social Science*, 588:40–51.

Badr, G. M. (1978). Islamic law: its relation to other legal systems. *The American Journal of Comparative Law*, 26(2):187–198.

Bahill, A. A. and Henderson, S. J. (2005). Requirements development, verification, and validation exhibited in famous failures. *Systems Engineering*, 8:1–14.

Bhootra, B. L. (2006). Forensic pathology services and autopsy law of Qatar. *Journal of Clinical Forensic Medicine*, 13(1):15–20.

Bittner, K. and Spence, I. (2002). *Use case modeling*. Addison-Wesley, USA.

Booch, G., Rumbaugh, J., and Jacobson, I. (2005). *Unified Modeling Language User Guide, The (2nd Edition) (Addison-Wesley Object Technology Series)*. Addison-Wesley Professional.

Braz, F., Fernandez, E., and VanHilst, M. (2008). Eliciting security requirements through misuse activities. In *Proceedings of the 2008 19th International Conference on Database and Expert Systems Application*, pages 328–333.

Breaux, T. and Antón, A. (2008). Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34:5–20.

Breaux, T. D. (2009). Exercising due diligence in legal requirements acquisition: A tool-supported, frame-based approach. In *Proceedings of the 17th IEEE International Requirements Engineering Conference (RE'09)*, pages 225 –230.

Breaux, T. D., Antón, A. I., and Spafford, E. H. (2009). A distributed requirements management framework for legal compliance and accountability. *Computers & Security*, 28(1-2):8–17.

Breaux, T. D., Vail, M. W., and Antón, A. I. (2006). Towards regulatory compliance: extracting rights and obligations to align requirements with regulations. In *Proceedings of the 14th IEEE International Requirements Engineering Conference*, pages 46–55.

Burrows, M., Abadi, M., and Roger, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36.

Cannataci, A. (2009). Privacy, technology law and religions across cultures. *Journal of Information Law & Technology*, 1.

Coulin, C. R. (2007). *A situational approach and intelligent tool for collaborative requirements elicitation*. PhD thesis, University of Technology, Sydney and Université Paul Sabatier (Toulouse III), France.

Cysneiros, L. and do Prado Leite, J. (2004). Nonfunctional requirements: from elicitation to conceptual models. *IEEE Transactions on Software Engineering*, 30(5):328 – 350.

Dano, B., Briand, H., and Barbier, F. (1997). A use case driven requirements engineering process. *Requirements Engineering*, 2:79–91.

Davis, G. B. (1982). Strategies for information requirements determination. *IBM Systems Journal*, 21(1):4–30.

Davison, J. and Fitzgerald, J. (2010). *Technical due diligence in Sweden*. Master of science thesis, The School of Architecture and the Built Environment, the Royal Institute of Technology (KTH), Sweden.

Desai, M. E. (2010). I want to ask whether it is ok to use Facebook as there are a lot of anti-Islamic pages and groups on it? Some of my friends still use facebook even after that event name. Available at *http://www.askimam.org/fatwa/fatwa.php?askid=eadca6a452a8295ec2ca96a7661bc30c/*.

Escalona, M. J. and Koch, N. (2004). Requirements engineering for web applications - a comparative study. *Journal of Web Engineering*, 2(3):193–212.

Fayad, M. E. (1997). Software development process: a necessary evil. *Communications of the ACM*, 40(9):101–103.

Fernandez, E. B., VanHilst, M., Petrie, M. M. L., and Huang, S. (2006). Defining security requirements through misuse actions. In *IFIP Workshop on Advanced Software Engineering*, pages 123–137.

Firesmith, D. (2003). Security use cases. *Journal of Object Technology*, 2(3):53–64.

Glinz, M., Berner, S., Joos, S., Ryser, J., Schett, N., and Xia, Y. (2001). The ADORA approach to object-oriented modeling of software. In Dittrich, K., Geppert, A., and Norrie, M., editors, *Advanced Information Systems Engineering*, volume 2068 of *Lecture Notes in Computer Science*, pages 76–92.

Goforth, C. R. and Goforth, R. R. (2001). Technology due diligence – the need for and benefits of technology assessment in connection with investment in high-tech companies. *Rutgers Computer and Technology Law Journal*, 27:165–204.

Goguen, J. A. (1996). Formality and informality in requirements engineering. In *Proceedings of International Conference on Requirements Engineering*, pages 102–109.

Goguen, J. A. and Linde, C. (1993). Techniques for requirements elicitation. In *Proceedings of IEEE International Symposium on Requirements Engineering*, pages 152 –164.

Gole, W. J. and Hilger, P. J. (2009). *Due Diligence: An M&A Value Creation Approach*. John Wiley and Sons, New York.

Gregoriades, A. and Sutcliffe, A. (2005). Scenario-based assessment of nonfunctional requirements. *IEEE Transactions on Software Engineering*, 31(5):392 – 409.

Hall, T., Beecham, S., and Rainer, A. (2002). Requirements problems in twelve software companies: an empirical analysis. *IEE Proceedings Software*, 149(5):153 – 160.

Hassan, W. and Logrippo, L. (2008). Requirements and compliance in legal systems: a logic approach. In *Requirements Engineering and Law, 2008. RELAW '08.*, pages 40 –44.

Haumer, P., Heymans, P., Jarke, M., and Pohl, K. (1999). Bridging the gap between past and future in RE: A scenario-based approach. In *Proceedings of IEEE International Symposium on Requirements Engineering*.

Hayat, M. A. (2007). Privacy and Islam: from the Quran to data protection in Pakistan. *Information & Communications Technology Law*, 16(2):137–148.

Hickey, A. M. and Davis, A. M. (2003). Requirements elicitation and elicitation technique selection: a model for two knowledge-intensive software development processes. In *Hawaii International Conference on System Sciences (HICSS)*, pages 96–105.

Hickey, A. M. and Davis, A. M. (2004). A unified model of requirements elicitation. *Journal of Management Information Systems*, 20(4):65–84.

Holbrook, H. (1990). A scenario-based methodology for conducting requirements elicitation. *ACM SIGSOFT Software Engineering Notes*, 15(1):95–104.

Holtzblatt, K. and Beyer, H. R. (1995). Requirements gathering: the human factor. *Communications of the ACM*, 38(5):31–32.

Hussein, S. (2010). World's leading Halal search engine makes Arabic content better accessible. Available at *http://www.zawya.com/Story.cfm/sidZAWYA20100714055733*.

IEEE (1990). IEEE standard glossary of software engineering terminology. *IEEE Std 610.12-1990*.

Jackson, M. (1997). The meaning of requirements. *Annals of Software Engineering Special Issue on Software Requirements Engineering*, 3:5–21.

Jacobson, I. (1992). *Object-oriented Software Engineering*. ACM, USA.

Jacobson, I. (2004). Use cases - yesterday, today, and tomorrow. *Software and Systems Modeling*, 3:210–220.

Jin, Z. (2006). Revisiting the meaning of requirements. *Journal of Computer Science and Technology*, 21(1):32–40.

Jorgensen, R. (2001). The oxymoron of use case requirements. *INCOSE INSIGHT Newsletter*, 4(2):21–22.

Kadivar, M. (2003). An introduction to the public and private debate in Islam. Part I: public/private: the distinction. *Social Research*, 70(3):659–680.

Kamali, M. H. (1993). Fundamental rights on the individual: an analysis of Haqq (right) in Islamic law. *American Journal of Islamic Social Sciences*, 10(3):340–366.

Kamali, M. H. (2003). *Principles of Islamic Jurisprudence*. The Islamic Texts Society, UK.

Kamalrudin, M., Grundy, J., and Hosking, J. (2010). Managing consistency between textual requirements, abstract interactions and essential use cases. In *Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual*, pages 327 –336.

Kettani, H. (2010). 2010 World Muslim population. In *Proceedings of the 8th Hawaii International Conference on Arts and Humanities*, USA.

Khan, M. A. M. (1997). Islam as an ethical tradition of international relations. *Islam and Christian-Muslim Relations*, 8(2):173–188.

Kotonya, G. and Sommerville, I. (1998). *Requirements Engineering: Processes and Techniques*. John Wiley & Sons, USA.

Kruchten, P. (2003). *The Rational Unified Process: An Introduction*. Addison-Wesley, USA.

Lee, W. J., Cha, S. D., and Kwon, Y. R. (1998). Integration and analysis of use cases using modular Petri nets in requirements engineering. *IEEE Transactions on Software Engineering*, 24(12):1115 –1130.

Leffingwell, D. and Widrig, D. (2000). *Managing Software Requirements: A unified approach*. Addison-Wesley, USA.

Lehman, M. (1991). Software engineering, the software process and their support. *Software Engineering Journal*, 6(5):243 –258.

Lombardi, C. B. and Brown, N. J. (2006). Do constitutions requiring adherence to Shari'a threaten human rights? how Egypt's constitutional court reconciles Islamic law with the liberal rule of law. *American University International Law Review*, 21:379–435.

Longjun, H., Changgen, J., and Caiying, Z. (2010). The research of requirements elicitation for project. In *Second International Conference on Multimedia and Information Technology (MMIT)*, volume 2, pages 302 –305.

Lucia, A. D., Fasano, F., Oliveto, R., and Tortora, G. (2007). Recovering traceability links in software artifact management systems using information retrieval methods. *ACM Transactions on Software Engineering and Methodology*, 16(4).

Lund, B. R., Andersson, M., and Bergstrand, J. (1996). A hierarchical use case model with graphical representation. In *Proceedings of the IEEE Symposium and Workshop on Engineering of Computer Based Systems*, pages 270 –277.

Maali, B., Casson, P., and Napier, C. (2006). Social reporting by Islamic banks. *Abacus*, 42(2):266–289.

Maghaireh, A. (2008). Shariah law and cyber-sectarian conflict: How can Islamic criminal law respond to cyber crime? *International Journal of Cyber Criminology*, 2(2):337–345.

Maiden, N. and Robertson, S. (2005). Developing use cases and scenarios in the requirements process. In *Proceedings of the 27th international conference on Software engineering*, pages 561 – 570.

Massey, A. K., Otto, P. N., and Antón, A. I. (2008). Aligning requirements with HIPAA in the iTrust system. In *International Requirements Engineering, 2008. RE '08. 16th IEEE*, pages 335 –336.

Massey, A. K., Otto, P. N., Hayward, L. J., and Antón, A. I. (2010). Evaluating existing security and privacy requirements for legal compliance. *Requirements Engineering*, 15(1):119–137.

Maududi, S. A. A. (1987). *The meaning of the Quran*. Islamic publications (PVT) LTD, Pakistan.

McDermott, J. P. and Fox, C. (1999). Using abuse case models for security requirements analysis. In *ACSAC*, pages 55–65. IEEE Computer Society.

Moghul, U. (1991). Approximating certainty in ratiocination: how to ascertain the Illah (effective cause) in the Islamic legal system and how to determine the ratio decidendi in the Anglo-American common law. *The Journal of Islamic Law*, pages 15–16.

Mohammad, F. (2001). Review: analogical reasoning in Islamic jurisprudence: a study of the juridical principle of Qiyas, by Ahmad Hasan. *Journal of Law and Religion*, 15:pp. 359–362.

Nambisan, S. (2002). Software firm evolution and innovation-orientation. *Journal of Engineering and Technology Management*, 19(2):141 – 165.

Nasr, E., McDermid, J., and Bernat, G. (2002). Eliciting and specifying requirements with use cases for embedded systems. In *Proceedings of the Seventh IEEE International Workshop on Object-Oriented Real-time Dependable Systems (WORDS 2002)*, pages 350 –357.

Nebut, C., Fleurey, F., Le Traon, Y., and Jezequel, J.-M. (2006). Automatic test generation: a use case driven approach. *IEEE Transactions on Software Engineering*, 32(3):140 – 155.

Norman, A. A., Nasir, M. H. N. M., Fauzi, S. S. M., and Azmi, M. (2009). Consumer acceptance of RFID-enabled services in validating Halal status. In *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*, pages 911 –915.

Nunes Leal Franqueira, V. (2009). *Finding multi-step attacks in computer networks using heuristic search and mobile ambients*. PhD thesis, The University of Twente. CTIT Ph.D.-thesis series No. 09-154.

Nuseibeh, B. and Easterbrook, S. (2000). Requirements engineering: a roadmap. In *Proceedings of the Conference on The Future of Software Engineering*, ICSE '00, pages 35–46.

Obbink, H., Kruchten, P., Kozaczynski, W., Postema, H., Ran, A., Dominick, L., Kazman, R., Hilliard, R., Tracz, W., and Kahane, E. (2001). Software architecture review and assessment (SARA) report version 1.0. Research report, SARA W.G.

Oberg, R., Probasco, L., and Ericsson, M. (1998). Applying requirements management with use cases: Rational software. Technical paper TP505 (version 1.4).

Osterweil, L. (1987). Software processes are software too. In *Proceedings of the 9th international conference on Software Engineering*, ICSE '87, pages 2–13.

Otto, P. N. and Antón, A. I. (2007). Addressing legal requirements in requirements engineering. *15th IEEE International Requirements Engineering Conference*, pages 5–14.

Paetsch, F., Eberlein, A., and Maurer, F. (2003). Requirements engineering and agile software development. In *WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on In IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pages 308 – 313.

Park, J., Jin, H., Kim, K., and JJ, K. (2009). A study on real-time progress management system modeling using goal and scenario based requirements engineering. In *Fourth International Conference on Computer Sciences and Convergence Information Technology*, pages 262 –265.

Park, J. and Sandhu, R. (2004). The $UCON_{ABC}$ usage control model. *ACM Transaction on Information and System Security*, 7(1):128–174.

Parkin, S., Moorsel, A. A., and Coles, R. (2009). An information security ontology incorporating human-behavioural implications. In *SIN '09: Proceedings of the 2nd International Conference on Security of Information and Networks*, pages 46–55.

Pauli, J. J. and Dianxiang, X. (2006). Integrating functional and security requirements with use case decomposition. *11th IEEE International Conference on Engineering of Complex Computer Systems*, pages 57–66.

Pfleeger, S. L. and Pfleeger, C. P. (2009). Harmonizing privacy with security principles and practices. *IBM Journal of Research and Development*, 53:273–289.

Potts, C., Takahashi, K., and Antón, A. I. (1994). Inquiry-based requirements analysis. *IEEE Software*, 11(2):21 –32.

Pouloudi, A. and Whitley, E. A. (1997). Stakeholder identification in inter-organizational systems: gaining insights for drug use management systems. *European Journal of Information Systems*, pages 1–14.

Ralyté, J., Rolland, C., and Plihon, V. (1999). Method enhancement with scenario based techniques. In Jarke, M. and Oberweis, A., editors, *CAiSE*, volume 1626 of *Lecture Notes in Computer Science*, pages 103–118.

Rational Software Corporation (2005). *Documentation of the Rational Unified Process in Rational Method Composer V 7.5.0.1*.

Rubin, K. S. and Goldberg, A. (1992). Object behavior analysis. *Communications of the ACM*, 35(9):48–62.

Rumbaugh, J. E. (1994). Getting started: using use cases to capture requirements. *Journal of Object-Oriented Programming (JOOP)*, 7(5):8–12, 23.

Schenker, J. G. (2002). Gender selection: cultural and religious perspectives. *Journal of Assisted Reproduction and Genetics, Netherlands*, 19(9):400–410.

Serour, G. I. (1993). Bioethics in artificial reproduction in the Muslim world. *Bioethics*, 7(2-3):207–217.

Shehaby, N. (1982). Illa and Qiyas in early Islamic theory. *American Oriental Society*, 102(1):27–46.

Sikora, E., Daun, M., and Pohl, K. (2010). Supporting the consistent specification of scenarios across multiple abstraction levels. In Wieringa and Persson (2010), pages 45–59.

Sindre, G. and Opdahl, A. L. (2000). Eliciting security requirements by misuse cases. In *Proceedings 37th International Conference on Technology of Object-Oriented Languages and Systems. TOOLS-Pacific 2000*, pages 120–131.

Sindre, G. and Opdahl, L. (2005). Eliciting security requirements with misuse cases. *Requirement Engineering*, 10(1):34–44.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania law review*, 154(3):477–564.

Solove, D. J. (2008). The new vulnerability: data security and personal information. In Chander, A., Gelman, L., and Radin, M. J., editors, *Securing Privacy in the Internet Age*, pages 111–132. Stanford University Press.

Sowa, J. F. and Majumdar, A. K. (2003). Analogical reasoning. In *Conceptual Structures for Knowledge Creation and Communication*, LNAI 2746.

Sutcliffe, A., Maiden, N., Minocha, S., and Manuel, D. (1998). Supporting scenario-based requirements engineering. *IEEE Transactions on Software Engineering*, 24(12):1072–1088.

Thomborson, C. (2010). A framework for system security. In Stavroulakis, P. and Stamp, M., editors, *Handbook of Information and Communication Security*, pages 3–20.

van Lamsweerde, A. and Willemet, L. (1998). Inferring declarative requirements specifications from operational scenarios. *IEEE Transactions on Software Engineering*, 24(12):1089 –1114.

Čejka, M. (2009). Making the Internet Kosher. Orthodox (Haredi) Jews and their approach to the world wide web. *Masaryk University Journal of Law and Technology*, 3(1):99–109.

Vinnicombe, T. (2010). AAOIFI reporting standards: measuring compliance. *Advances in Accounting*, 26(1):55–65.

Wahli, U., Irani, M., Negrello, A., Palma, C., and Smith, J. (2006). *Rational business driven development for compliance*. IBM Redbook.

Wieringa, R. and Persson, A., editors (2010). *Requirements Engineering: Foundation for Software Quality, 16th International Working Conference, REFSQ 2010, Essen, Germany, June 30 - July 2, 2010. Proceedings*, volume 6182 of *Lecture Notes in Computer Science*.

Yilmaztürk, N. (2005). Good quality requirements in unified process. In Aurum, A. and Wohlin, C., editors, *Engineering and Managing Software Requirements*, pages 373–403.

Zafar, S. (2010). Pakistan blocks access to youtube in internet crackdown. Available at http://www.bbc.co.uk/news/10130195.

Zainul, N., Osman, F., and Mazlan, S. H. (2004). E-commerce from an Islamic perspective. *Electronic Commerce Research and Applications*, 3(3):280–293.

Zowghi, D. and Coulin, C. (2005). Requirements elicitation: a survey of techniques, approaches, and tools. In Aurum, A. and Wohlin, C., editors, *Engineering and Managing Software Requirements*, pages 19–46.

Zuser, W., Heil, S., and Grechenig, T. (2005). Software quality development and assurance in RUP, MSF and XP: a comparative study. *ACM SIGSOFT Software Engineering Notes*, 30:1–6.