CHAPTER II

LITERATURE REVEIEW

2.1 Introduction

Many studies have been proposed to explain and verify security functionality of smart phone. Although, the literature covers a wide variety of security functionality smart phone, this review will focus mainly on three important factors which may emerge repeatedly throughout the literature review. The factors would be the themes such as mobile security, mobile security functionality as well as the awareness security users. Although, the literature presents these themes in a variety of contexts, this study will primarily focus on their application in security functionality of smart phone in order to protect the users from threats and others risks due to daily usage.

2.2 Mobile security

In this section, more discussion is employed for the statistics of the mobile phone usage and also presents studies which are related to the security functions in mobile phones. Mobile security includes the protection of personal data as well as confidential information which are stored in all mobile devices such as smart phones, tablets, laptops and other portable computing devices.

Definition: Mobile security is the protection of all devices such as smart phones, tablets, and laptops, including protecting personal and business information that stored on mobile devices, and protecting the networks connection from threats and vulnerabilities. The world of mobile security covers various issues such as protecting mobile devices from malware threats, risks and securing mobile devices. Companies are working hard to control sensitive information that could be jeopardized their data from unauthorized access or loss because of its use on various mobile devices.

2.2.1 Mobile security threat

There is a type of threats depending on devices or the amount of information stored on the device, as well as the ability of installed applications to access that information. Sometimes, downloading applications from unreliable sources is considered a threat to mobile devices, "Malicious apps" may seem fine on a download site, but they are specifically designed to commit fraud. Their software based threats can compromise the data on the mobile devices. Mobile security threats include everything starting from the forms of malware and spyware to the potentiality of unauthorized access to a device's data, particularly in the case of accidental loss or theft of the device. Mobile malware and spyware security threats can access a device's private data without user's knowledge or consent and can perform malicious actions, such as malware is considered software that performs malicious actions while installed on your phone. Without the users' knowledge, Spyware is designed to collect or use private data without users' knowledge or approval. Privacy threats may be caused by applications that are not necessarily malicious, but by gathering or using sensitive information. Sometimes the threat comes from the user in

case of negligence of the mobile device when not focusing on how to protect the device and failing to understand the dangers surrounding it. At the present time, business is conducted via the mobile devices; this means the threat does not come only from the malware software but also from the users themselves. The users are considered a cause for the loss or theft of their devices. Because there are some of the attackers, keeping tabs on the user through mobile devices and exploit the weaknesses of the existing setups. These threats can disrupt the operation of the mobile devices, and transmit or modify user data. The first target is data as some user kept sensitive data like credit card numbers, private information. The second target is identity as every mobile device can transmit information related to the owner of the mobile phone; an attacker may want to steal the identity of the owner of the mobile device to commit other offenses. Hence, the users should pay attention to these threats.

2.3 Mobile security functionalities

In this section, the security functionality is divided into many classifications with an explanation to each one. All these classifications are called authentication mechanisms.

2.3.1 Personal Identification Number (PIN)

Nowadays, the most commonly used authentication mechanisms are passwords, and this is because they are considered the easiest way to be used compared to the rest of the authentication available methods, but password is considered less safe roads because

the users in their choice of words are weak or may use the same password in many accounts (Feng et al., 2012).

Definition: PIN is a numeric password, can use it as an authentication method between the user and the system used in the smart phone. Main work for PIN is to protect Subscriber Identity Module (SIM). In case of theft or loss of smart phones, it can prevent an unauthorized user to use SIM card in another phone, for example if you lose your SIM card and if someone tries to use it on another device, it cannot be operated unless the SIM PIN is inserted correctly.

In one year, security measures were stolen amounted to more than 1 million mobile phones users in Europe. The process of theft and other unwanted incidents can be prevented by protecting user phones with special PIN code. The (PIN) function is to protect the users from an unauthorized usage for the Subscriber Identity Module (SIM card). In recent years, with the advancement in technology, it was discovered that users have many ways to protect their devices called "method authentication" or "biometric authentication", where the PIN authentication is based on some codes, alphabets, patterns or features which the users is familiar with. Biometrics is based on what the user can utilize such as; Fingerprint, voice biometrics, facial recognition (Stewart and Mikael, 2006).

A study by Furnell et al., (2000) emphasized on the user's attitude towards different various authentication. It reveals that 90% of the computer users such as smart

phones users prefer to use passwords as authentication method. While 68% to 67% accepted the authentication method such as voice verification and fingerprint recognition.

In 2002, a survey was conducted by Clarke et al and found that 89% of the respondents knew about the PIN, but only 56% acknowledged and used it. It means two-thirds of respondents do not use PIN.

Furthermore, Clarke found that majority of the users depend on the protection of (SIM) by use protection of (PIN). The majority of the users show a poor awareness toward security functionality. Respondents are unaware of any security functionality which is available in the market.

Stewart and Mikael (2006) conducted a study to examine the awareness of the security functions of mobile phone. The study targeted 97 Swedish students' awareness security where half of them were less than 30 years. Participants were 16% of "Early adopters" and 46% of "Laggards". `Respondents did not have the knowledge in any security functionality other than the PIN. The Awareness of security functionality was not good. Were available two levels of security, the first level to protect the SIM card from unauthorized usage by using PIN code. While the second level for protecting the phone security by using password code. 82% of users' usage of the PIN code was through authentication method, while 15% of users' adoption of the phone security code was used as authentication method. 33% of users did not use phone security codes.

2.3.2 Biometric Authentication

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure) which forms a definition for Biometrics and refers to the automatic identification of a person based on physiological or behavioral characteristics.

In this section, a definition of biometric authentication is given. The main reason for using biometric is to protect smart phone data. Unfortunately, smart phone thefts are on a rise where most people become victims of theft of smart phones. Using biometrics protects the data on smart phone because it serves as a protection shield in order to prevent access into information that exists in the smart phone.

Definition by Johan:

"Biometric is one of the authentication methods, which work on determine the identities of the people through several properties. These techniques can be divided biometrics into two main groups: the Physiological or Behavioral. Physiological biometric method looks a physical feature of body, while behavioral biometric method is dependent on what you do in your daily life" (Johan, 2005).

Bhattacharyya et al., (2009) suggested that biometric authentication can be divided into two main classes:

A-*" Physiological are related to the shape of the body and thus it varies from person to person Fingerprints, Face recognition, hand geometry and iris recognition are some examples of this type of Biometric."*

B- "Behavioural are related to the behaviour of a person. Some examples in this case are signature, keystroke dynamics and of voice. Sometimes voice is also considered to be a physiological biometric as it varies from person to person.

2.3.2.1 Fingerprint recognition

This is the oldest authentication method among the other available authentication methods and is commonly used and very famous. It works on the analysis of fingerprints in order to identify the person. There are two techniques in order to analysis the fingerprints; the first one is by scanning optically the finger of a person, and the other method is through the usage of electrical charges. Each imprint has some characteristics, such as curves, dendrites, and delta. The main characteristic of the fingerprint does not change where the gap in this method is a clone fingerprint, for example, thefts can be successfully done by imitating the fingerprint by using silicon. Fingerprints are usually used in many organizations (Johan, 2005).

Debnath et al., (2009) defined fingerprint as

"*A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar or digits (fingers and toes) or plantar skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal ". The traditional method uses the ink to get the finger print onto a piece of paper. Now in modern approach, live finger print readers are used .These are based on optical, thermal, silicon or ultrasonic*

principles. It is the oldest of all the biometric techniques. Optical finger print reader is the most common at present".

2.3.2.2 Facial recognition

Debnath et al., (2009) defined facial recognition:

"A *facial recognition technique is an application of computer for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is the most natural means of biometric identification. Facial metric technology relies on the manufacture of the specific facial features (the system usually look for the positioning of eyes, nose and mouth and distances between these features)".*

2.3.2.3 Voiceprint recognition

This method is built on human voice. It is done by using some frequency analysis of the voice. This analysis is based and recognized on to the way users speak and not based on what they express. It is less accurate than other authentication methods, because this authentication method can be easily fooled by recording someone's voice (Johan, 2005).

This technique can be divided into different classifications based on the type of authentication domain.

• Fixed text method

This technique is operated by requesting the speaker to say one word then it is recorded during programming on the system.

• The text dependent method the system prompts

This technique depends on the user way of saying a specific word or phrase, and then computed on the basis of the user's fundamental voice pattern.

• The text independent method:

This technique doesn't need to say any specific word or phrase. It works by matching the user voice on the basis of the fundamental voice patterns irrespective of the text used in the process (Angle, 2005).

2.3.2.4 Signature recognition

Signature analysis is a biometric authentication method; the user signed on a display device by touch. The information that is calculated to authenticate are the time the user takes to sign and the pen pressure. Possibilities are very high to restore the same signature by someone else (Johan, 2005).

2.3.3 IMEI Number

International Mobile Equipment Identity - IMEI: Is the definition of a special phone number, a unique number for each mobile phone which cannot be repeated in any other phone features in the world. This number is considered as an identification number for the smart phone, because retrieving accurate information should be from the same phone.

In order to be recognized by this IMEI number, the user can read it from the paper affixed to the back of the device, which consists of 15 digits and the user can also know more about the road code * # 06 # (from left to right) and the number that appears

on the phone screen enables the usefulness of the lock number of the phone in case of theft, so the SIM card cannot be penetrated and used by unauthorized persons.

The ETSI (European Telecommunications Standards Institute) **defined International Mobile Station Equipment Identity (IMEI)** as: *"An International Mobile Station Equipment Identity is a unique number which shall be allocated to each individual mobile station equipment in the GSM system and shall be unconditionally implemented by the MS manufacturer". And general say "As described in GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purpose"*

"The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the GSM system cannot or no longer be tolerated for technical reason" (ETSI, 2000).

2.4 Types of Security

They are everywhere iPhones, Androids, and Blackberrys. Whether call them smartphones. They are different from traditional phones in that they are also microcomputers, they have an operating system, can run a variety of software applications, and provide access to the web. Most new smartphones provide one or more types of wireless network connectivity, be it 3G, 4G, Wi-Fi, and/or Bluetooth.

Unfortunately, today's smartphone users are in a situation strikingly similar to that faced by computer users fifteen years ago. Security resources for smartphones are very limited and not fully developed. As a result, most smartphones lack the level of security. Meanwhile, so the complexity of smartphones continues to grow along with the number and types of network-borne threats. This makes smartphones both an easy target for hackers and malware. When using smart phone security the most important thing can do to protect smartphone is to understand how to use it safely. There are many types of security items or security services in smartphones, such as password, data encryption. That mean types of security are the items or services can by this services protected smart phones.

2.5 Security Attitude

Attitude is considered a hypothetical construct that the users of smart phones express an individual's degree of like or dislike for the service (Ahmed and Arash, 2011). Attitude is a good predictor of human intention and behavior. Attitude is one of the determining factors in predicting people's behavior. That is to say by understanding an individual's attitude towards something, one can predict with high precision the individual's overall pattern of behavior to the object (Kutluca, 2011). Attitudes -refer to the degree to which a person has a favorable or unfavorable evaluation of the behavior of interest. It entails a consideration of the outcomes of performing the behavior (Maria, 2014). The primary goal for any organization is to create security awareness program in

order to change the users' attitude towards information security. Changing the attitude creates ways to change the behavior of the users.

Attitude governs people acceptance of the technologies or service as well as their practices to accept or apply certain features to protect their data. Ahmed and Arash (2011) conducted a study to review the users' attitudes and opinions toward security practices when using their mobile devices. The respondents think that PIN is an adequate procedure for their devices, also 32.8% of them agree that mobile devices need to increase security features. While 19% of the users agree and 2.9% strongly agree on the statement that by paying more money, users get more security for their device.

Esmaeili (2014) findings revealed that users' attitude toward the adoption of security technology was affected primarily by their perception of a possible security breach severity and their perceptions toward the usefulness of these security technologies. If the users thought that the security breaches would affect them severely, and/or if they believed that using the security technologies on their smartphones would be useful, then they tended to have more positive attitudes about using these technologies on their smartphones. This study found no significant relationship between users' perception of the ease of using a security breach and their attitudes toward using security technology on their smart phones.

2.6 Security Behavior

Behavioral intention refers to the motivational factors that influence a given behavior where the stronger the intention to perform the behavior, the more likely the behavior will be performed (Maria, 2014).

Security awareness is critical for organizations to protect them from any threats. Any organization needs awareness security program to target the user behaviors. Moreover, organizations need to create awareness of the factors that cause threats and how to prevent such threat to their employees (Kutluca, 2011). There are few research studies related to security behavior of smart phone users and how the behavior can be modified to practice security countermeasures. Past incidents may put focus on the vital behaviors to be targeted in a particular organization, as past incidents may change the behavior to be better.

This may include the behaviors that led directly to a past incident or the recovery behaviors that the organization needs to get back on the right track after committing mistakes. Focusing on the types of risks that can't be fully covered by technical solutions leads to focus more on the policy, procedure and education which can highlight vital behaviors (Spitzner, 2012).The primary purpose of the security awareness is to change behavior but positively. Security awareness professionals should focus not only on the big picture of what they want to achieve, they also must identify the behaviors they wish to change before they start trying to change them (Winkler and Manke, 2013).

2.7 Security Training

Security awareness training is a process for educating users about policies and procedures of information security. Regular training is particularly necessary in organizations, employees and all users' devices mobile. Security awareness training is also important for students, faculty and staff to understand the importance of the security system and to ensure that each individual understands his/her responsibilities.

Training is defined in NIST as follows:" *The training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus on an individual's attention on an issue or set of issues*". The skills acquired during training are built upon the awareness foundation. Training strives to produce relevant and needed security skills and competencies.

Training: This is more formal and has the goal of building knowledge and skills to help employees to do their jobs in a way that will not compromise a state's IT resources. In training, participants are expected to take an active role and may be asked to engage in exercises directed to help them applying the concepts introduced in training. The relationship between awareness and training is that awareness is the foundational level upon which training efforts can be rolled-out.

2.8 Security Awareness Users

security awareness mean understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within systems. There are three elements to protecting information:

Confidentiality: Protecting information from unauthorized disclosure to people or processes.

Availability: Defending information and resources from malicious, unauthorized users to ensure accessibility by authorized users.

Integrity: Assuring the reliability and accuracy of information and IT resources.

Also can risk mitigation through:

•Awareness of confidentiality, availability, and integrity risks that face the business

•Awareness of vulnerabilities that affect systems users.

Security awareness is a core component of an information security program. All organizations rely on their members as a crucial line of defense to keep their information and systems secure. Security awareness is considered an individual responsibility that needs a sufficient understanding to comply with policies. A good security awareness program should educate employees and users about information security on mobile devices. All users like employees or students should receive information security about mobile devices that help them to discover a security threat. The purpose of awareness is

to focus attention on security, the threats, and vulnerabilities of mobile device and recognition of the need to protect data, information and systems.

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is defined in NIST as follows:

"*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize security concerns and respond accordingly".*

It is important to have sufficient knowledge of the usage of computer where users must be fully equipped to understand the way computers function and how data are saved to avoid risk and hacking, because mobile devices are inherently insecure. Many users seldom take precautions to protect their phones or data.

Iosif and Gorazd (2010) conducted a survey to elaborate more the users' security perceptions regarding mobile phone usage. The survey was on 780 students in the University of Ioannina. The findings reveal that users still lack the knowledge to protect their hand phones as the authors believe that necessary steps should be taken to protect phones or data from an unauthorized access.

Frank and Claudia (2010) revealed that the analysis of the security level was very low due to low security awareness among users. Another reason can be the low acceptance of the authentication based methods. The total number of respondents who participated in the survey were 548 people, 55 % of them were between 18 to30 years old.

The results also indicated that the majority of the users are using a mobile phone to save their personal data and there are 13% of them using password or PIN to protect their hand phones during operational mode that is when the phone is in standby mode.

The empirical study was conducted on a sample of 7,172 students, who are studying in 17 universities in ten European countries. The purpose of this study is to assess the levels of users toward the security and awareness of the mobile phone communication. This study reveals that there are some users who may face an increase in the security risks because they feel that mobile phone communication can be more secure (Iosif, 2011).

2.9 Smartphone Security Awareness

Mubarak and Ali (2013) revealed that there is a lack of awareness on smartphone security. The majority did not know if their smartphones were hacked as it is sometimes difficult for users to know if their smartphone have been tampered with or hacked. In addition, the findings indicated that almost half of the respondents did not know for whom to report in case of an incident as 48% answered they did not know exactly where to report to if any incident occurs.

According to a study conducted by Lee et al., (2012) credibility, personalization, performance expectancy, social influence, flow, and promotion condition are considered the main factors that encourage users to use smart phones. These factors are taken into the user consideration while choosing a handset and credibility here refers to security, privacy and trust of customers. Ponemon institute conducted a security survey among US

customers. The findings indicated that the majority of the customers who use smart phones were not worried about the trustworthiness of downloaded mobile apps and hacking. In contrast, they were worried about location tracking and marketing abuse. The authentication mechanism used by the majority of smart phones users is PIN.

Although PIN based authentication is easy to use, many studies reveal that it needs a respected time to use alternate authentication system such as biometrics (Noam, 2011). Mobile threats are increasing at an alarming rate and have grabbed the attention of many companies working in the area to enhance the security. The threats faced by android phones are higher compared to Apple's iOS. The threat clusters identified for the android phones are exploitation of permissions granted to applications installed on phones to compromise Confidentiality, Integrity and Availability (CIA) (Asaf, 2009).

Studies also suggest that the users of smartphone are still not serious about password protection of their phones and very few of them apply encryption techniques on the phone stored data. The users are extensively using internet and social net- working applications so it is observed that they have many passwords on their browsers. This leads to internet fraud, identity theft and resulted in information theft. It is also observed that many users are not aware of the mobile security issues and inappropriate security practices that are prevailing among smartphone users (Appollonia, 2011).