CHAPTER 1

INDTRODUCTION

This chapter discusses the research rationale which consists of the background and followed with an overview of several previous methods for preserving user anonymity. The discussion continues with the theoretical framework, the conceptual framework, the statement of the problem, hypothesis, assumption, scope, and delimitation, as well as the importance of the studies.

1.1 Rationale

Recently a smart card is widely used for parking systems, financial transaction systems, etc. However, smart card still have several security vulnerabilities such as impersonation of legal users by extracting secret information stored in the smart card, off-line guessing password attack, and failure preserving user anonymity. Therefore, Das et al. [4] proposed a dynamic identity scheme for remote user authentication to secure the user's identity (ID), such that the adversary cannot manipulate the ID even he can intercept important parameters to forge the ID, guessing password and impersonating as legal user during login session. However, Lee et al.[9] shown that Das's scheme [4] completely insecure. Therefore, Lee et al.[9] proposed improvements against this vulnerability. The improvement proposed by Lee et al.[8] was on random number addition to authentication scheme during the login session. Unfortunately, Wen et al.[11] shows that the authentication scheme was not secure against offline password guessing and impersonation attack. Furthermore, the authentication scheme was improved by Lee et al.[8] using quadratic residue in the authentication phase. However Jung et al.[7] found that Lee's scheme [8] was not resistant against offline password guessing and impersonation attack. Furthermore, Lee's scheme cannot preserve the user anonymity [3].

The weakness of Lee's scheme [8] is the usage of user's identity for securing message authentication. Such that the adversary gets the dynamic user identity(DID_i), quadratic residue modulo n (C_i), and timestamp (T) sent by the user in the middle of communication during login session. The adversary can obtain the users identity (ID) using the intercepted data. Furthermore, the adversary extracts the value Mi and Ni from the smart card and uses these values along with the message authentication, then the adversary can obtain a user password and impersonate the legitimate user..

1.2 Theoretical Framework

Nowadays, smart cards are widely used for vital transactions such as ATM, E-tolls, parking cards, etc. Therefore, the scheme protects the smart card against offline password guessing and impersonation attack, and preserver user anonymity. First of all, to secure the smart card against offline password guessing and impersonation attack, it needs to preserve user anonymity, and protects the user ID against ID theft attack [4].Das et al. [4] introduce a dynamic identity-based remote user authentication to protect ID against theft attack. Basically, the authentication scheme using dynamic identity-based is a method for securing the value of ID using dynamic value during login session. However, the server needs to obtain ID from the dynamic identity of user authentication message user to verify whether the user is the legitimate one or not. After all authentication processes are successfully conducted and the server can verify that the user is the legitimate ones, then the user and the server need to generate a session key to secure the communication between the user and the server.

1.3 Conceptual Framework/Paradigm

The remote user authentication using a smart card requires efficient computation during an authentication session. On the other hand, authentication is necessary to reduce the probability of success in offline password guessing and impersonation attack conducted by the adversary. To provide efficient computation the proposed scheme uses keyed hash function and zero-knowledge proof [1].

The dynamic identity based authentication using smart card consists of registration phase, login phase, and verification phase. Only users registered in the system can access the resource in the server. Each user need to generate a password then sends it to the server, The server then generates authentication variable and stores into the smart card. The user can access the resource of the server after the user is verified by the server as the legitimate one; this process is conducted in the authentication phase. The first phase in authentication phase is the login phase. In the login phase users insert the cards into the machine, then input their user password into the machine. After they input the user password, the machine generates the authentication message and sends them to the sever. Furthermore, the server verifies the authentication message from the users. If the users are legitimate, then both the server and the users generate the session key for securing the further communication between them.

1.4 Statement of the Problem

Dynamic identity-based schemes have been proposed several times. Unfortunately, they are still vulnerable for password guessing and impersonating attacks, moreover, the schemes cannot preserve the user's anonymity such as Lee's scheme [8]. Lee's scheme [8] tries to preserve user anonymity using quadratic residue and the Chinese remainder theorem but Jung et al. [7]. has shown that Lee's scheme [8] fails to persevere user anonymity. Moreover, Jung indicates that [7] Lee's scheme [8] is vulnerable against password guessing and impersonation attack. The weakness of Lee's scheme is that uses the user identity for securing the authentication dynamic value and sent it to the server. The adversary obtain the authentication message from the user during the communication and use it along with the extracted secret values from the smart card to get the user's identity. The probability of success user identity guessing and impersonation is 1, and the probability of success password guessing is $1/2^{48}$. Thus, the security parameter depends on user identity. The success probability has shown the Lee's scheme completely insecure, securing the user identity is the major concern to strengthen the Lee's scheme.

1.5 Objective and Hypotheses

This research introduces a new scheme that attempts to improve or strengthen the security of Lee's scheme [8] against offline password guessing and impersonation attack. Moreover the proposed scheme could preserver the user anonymity while still preserving efficient computation. To strengthen Lee‘s scheme [8] against offline password guessing and impersonation attack, and preserve the user anonymity, the proposed scheme is introduced a zero-knowledge protocols. The zero-knowledge protocol is a method that users can prove to the server that they are legitimate ones without conveying any information apart from the fact that the user and server know the value [1]. It means that the user's secret is not known by the receiver, but the receiver can still authenticate the legitimate users. In the proposed scheme, the keyed hash function is used for creating the hash of user ID, password and the secret variables are known by both the users and the receivers. Thus, since the secret variable is secured by those two hash functions, and the adversary has stolen the smart card, the adversary cannot obtain the user identity and user password from the smart card.

1.6 Assumption

The server knows the user's identity while the user is in the authentication phase. The character used in the password is 0-9, a-z, A-Z, (!?@#$%&*/). The smart card used in the proposed scheme is a basic card version with a EEPROM (Electric Erasable PROM) capacity of 72 Kbytes and RAM (Random Access Memory) of 4 Kbytes.

1.7 Scope and Delimitation

The scope of this research is to increase the security level of Lee's scheme. Evaluation is conducted to check the level of the security of probability for obtaining DI and password.

1.8 Significance of the Study

Most authentication identity-based using smart cards still have a low-security level. Therefore, increasing the level of security of the scheme is a major concern. This research takes part in increasing the security level of the scheme. If the level of security is increased and secured, then vital transactions using smart cards such as ATM, E-tolls, parking cards, etc will be secure. The proposed scheme attempts to improve the security of Lee's scheme against password guessing, impersonation attack, and preserver the user anonymity while still preserving the efficient computation.