A SURVEY ON AN IMPROVED KEY AGREEMENT PROTOCOL FOR TELECARE MEDICINE SYSTEM

K. Prem Kumar[1,] P.Gayathri[2,]

Abstract -Data security is mainly used to protect the data from adversaries. It provides many techniques and methods that are applied to prevent unauthorized access. Telecare Medicine Information System (TMIS) is a medical equipment which is used to store the information about the patients. TMIS provides the security to the information by using the key agreement protocol. Lie et.al. pointed out that Zhang's protocol cannot avoid the off-line password guessing attack and fail to revocate missed / snatched smartcard. Hence, Liu et.al. proposed an improved protocol in which biometrics and smart card id concepts are used to solve these weaknesses. In the existing system, the attackers can hack the fingerprint by using Silicone gel. Also, if any malicious patients access the user account then it cannot be detected. In the proposed one, the system will send notification to the corresponding user regarding the invalid access. By using locking system the user can lock the account. The attacker could not access the account further. Then the user unlocks the account by answering the security questions which are provided at the time of registration. After that the user can change the password and use the account securely.

***Index Terms*— TMIS, smart card, biometrics, locking system**

I. INTRODUCTION

Data Security is defined as protection of data from invalid and malicious access. To provide security to the data, some data security technologies are used. The mainly used technologies are Disk encryption, Software versus hardware-based mechanisms for protecting data, Backups, Data masking, Data erasure etc. Each technology can be used to protect the data and avoid several attacks. Disk encryption used to encrypting the data for security. It collects data in the form of software or hardware. Because of this encryption, the attackers can face some difficulties to hack the information or data. In Software based mechanism, encryption of data is used for provide security. In Hardware based mechanism, some hardware devices can be used for provide security to the data. Back-up means storing the data in another source for recovery. If any attacks or problems happened, the data would be lost. In that situation, the lost data can be recovered by using Back-ups. In Data masking, the stored data are maintained in specified data base. Because of this, the system ensured that the sensitive data are not attacked by an unauthorized person. In Data erasure, the electronic data are erased which residing on hardware drive. Because of this, to ensure the stored data is not leaked when the database or asset reused.

TMIS means Telecare Medicine Information System. It can be used to store the information about the patients and maintains the data securely. It creates the relationship between patients and the doctors. The patients can easily know the medical details in anywhere. In this Telemedicine, there are three main categories: store-and-forward, remote patient monitoring and (real-time) interactive services. In store and forward, the medical data can be collected and covert into proper medical record. Then this data transmitted to doctor or medical specialist. In remote monitoring, patients can know or access the details about their health by remotely using various electronic devices. It helps patients to self monitor their health conditions. In real time interactive, the patients and provider can interact in real time which is less cost than the person clinical visit.

We need to protect the data from third parties. so we use an agreement protocol to provide security to Telecare Medicine Information System. In last few decades, TMIS faces some security problems such as offline guessing attacks, forward secrecy, man in the middle attack, denial of service attack etc. To avoid these problems, some techniques and methods are used. Provide smart card to the patients to access the account is help to provide the security to the data. Smart card is a pocket size card that can be embedded with IC.It can be used to stored the data and support for portable medical records. It is mainly used for identify the authorized user by using the information given by the user. For identification, it uses some cryptography algorithms.

In smart card generation there are four phases. Registration can be used to register the new user by entering the details about the patients. Next, log in phase which can be used to check whether the user is a valid user or not by

Manuscript received Feb, 2017.

***Prem Kumar.K**, Assistant Professor, Department of Computer Science and Engineering, M.Kumarasamy College of Engineering , Karur, Tamilnadu, 8012341480*

***Gayathri.P** PG scholar, Department of Computer Science and Engineering, M.Kumarasamy college of Engineering, Karur.Tamilnadu, 994334554.*

using the entered details in login phase. Then authentication phase can be used to authenticate the user. In password change phase if any unauthorized person accesses the account, the valid user can change the password by using this phase. With smart card, the locking system also provide for security purpose. If any unauthorized access or unwanted person accesses the patient's account, the patients can easily lock the account by using locking system. Because of this the attacker cannot access the account further more.

II. LITREATURE SURVEY

Ankita et al [1] suggested a new dynamic ID based authentication scheme that can used to avoid the offline password guessing attack and Denial of service attack. By using smart card, they change the login and password change phase efficient. The validity of the scheme can be checked by using BAN logic. There are four phases in this scheme namely registration, log in, Authentication and password change. The new user first register by entering details and personalized a smart card. In log in phase, the smart card is inserted into the terminal by the user and enter his ID and Password. Verification is done in this phase. Then user and server validate each other and fix the session key. By using the session key, An authentication is done. After this process only the user can access the account. So if any invalid user tries to access the account, It will not allow. The incorrect input can be identified easily in this scheme. The authorized user can never use the smartcard If she/he commits any mistake in password change phase. If it happens, the user will request for new smart card.

Kukki Arya et al[2] proposed the survey of Authentication schemes to provide security to the Telecare Medicine Information Systems. In this, There are three factors used namely username and password, smart card, Biometrics. The smart card authentication plays a major role in this scheme. After the login phase, the system ensure that the authorized user. So the server performs validation and authenticate the user by using the secret key which generated by the server. The secret key may changes from user to user as well as every login. If the authenticated process completed, the server would allowed the user to access the account. Stolen or lost smart card is major disadvantage in this scheme.

Zuowen tan[3] et al proposed an efficient scheme for smart card by applying biometrics information and hash function operations. Hash function provides the high efficiency and stronger authentication function. The execution time is getting reduce when using this scheme. The proposed scheme can resists many attacks like replay attack, stolen verifier attack, insider attack, impersonation attack etc. In this scheme, there are several hash functions used in each phases. In registration, two hash functions applied. During login and authentication, five hash function operations performed. In password updating one more hash function and one inverse function are used for operation. The disadvantage of this scheme is secure dynamic identity authentication.

Min Zhang et al [4] planned a scheme for security to telecare medicine information system by using sketch-based authentication. This scheme provides stronger security than other schemes. It is not only providing anonymity but also help for session key agreement. In this sketch scheme, there are two algorithms used. When registering the biometrics information of the user, the output us sketched by using sketch based algorithm. Then the second algorithm reconstructs the original biometric. In login phase, the entered biometric information compare with the reconstructed biometric. If it is match, then only it will allow the user to access the account. This scheme provides higher security and more concentrate in biometric. The disadvantage of this scheme is cost of the process.

Yang sun [5] developed a scheme for improving the efficiency of Telecare Medicine Information System. This scheme shows that Lu et.al scheme using the XOR operation in wrong way and some other flaws. So this scheme revises these flaws. The Security of the system is proved by BAN logic. In this scheme, chaotic map based cryptography is used. It is better than traditional cryptography. The chaotic scheme is mainly used for two party authentications. By using this smart card denial of access flaw can be controlled. Potential loophole of XOR operation is used here. Novel method is used here. There are two phases. In registration phase, the new user can enter the details. In login and authentication phase, create an authenticate key and session key for security. Those two keys are used for verify the details entered by the user. The disadvantage of this scheme is cost of the process and it is not panacea but it offers some security.

Zhang's et al provides authenticate agreement scheme with privacy protection for Telecare Medicine System for security purpose. But it cannot resists offline password attack and fails to provide stolen/lost smart card. To overthrown these weaknesses, Wenhao et al[6] proposed an improved authenticated protocol. This protocol can resolve the security problems and that can be proven by using pi calculus based formal tool Proverif. In this scheme, they can be generated unique Id for each smart card. If the smart card is lost/ stolen, the user can request for revocation of smart card to the server. Then the server accept the request and generate the new smart card with new id and update the details. When the adversary inserts the lost smart card into the terminal, it will check the smart card id. If it is not in the server, the server will not allow to access the account. It resists the offline password guessing attack, revocation of stolen/lost password. The disadvantage of this scheme is biometrics information can be identified by using silicone gel.

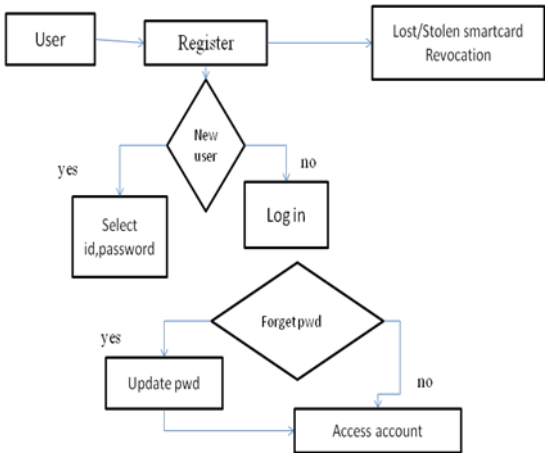
To overcome the weakness in the Mishra et al scheme, Zhang et al [7] proposed a three factor authenticated scheme. In this, chaotic map based cryptography used for privacy protection. There are five phases in this scheme. In initialization phase, server chooses master key, one way hash function and symmetric key cryptosystem. In registration phase, new user register first by using his/her details and the data stored into the smart card. By using the smart card, the user can access the account. In authentication phase, three factor authenticated key to be used. To design the three factor

authenticated key, several algorithms are used. Normally, one way hash function, RSA crypto system, chaotic maps are used in authentication phase. Here, Zhang et al used Elliptic Curve Cryptography for authentication phase. It is more suitable for authentication than the other algorithms. This scheme can resists various attacks and also suitable for practical applications.

Mehul[8] explained in his article about the notification alerts by using Notification Manager. Notification means a simple action can be created for intimate the access performed in the top of the activity. This simple Notification is used to inform that the message is attains regarding account. The android support V4 notification compact used here. Several methods are used for Notification creation. SetTicker() method is used to expo message like popup when alert attains. We can set no.of notifications by using setNumber() method. There are four steps involved in this process namely display notification, Update notification, Inbox style notification, Cancel notification.

III. PROBLEM DESCRIPTION

The Telecare Medicine Information System (TMIS) has created a connection by using telecommunication systems between the doctors at hospitals and patients at home. TMIS is making a difference by employing information and communication technologies to upgrade the feature of healthcare services. TMIS should be secured because the patient's valuable informations are recorded. So Zhang proposed an agreement protocol to provide security for TMIS. The Problems identified in Zhang's protocol are: cannot avoid the off-line password guessing attack and fail to revocate missed / snatched smartcard. To overthrown these weaknesses Wenhao Liu et al suggested an improved authenticated key agreement protocol for TMIS. In that protocol they use biometric keys to find solution for the security problems. Furthermore, they afford the imitation results of our scheme for the formal security verification, using applied pi calculus based on ProVerif tool.



However, biometrics keys can be identified by using silicone gel. So the attackers can easily guess the passwords. In proposed one, the system send notification to the corresponding user regarding the invalid access. The user locks the account by using locking system and hence the attacker could not access further.

IV. CONCLUSION

The telecare medical information system promotes the patients gain health monitoring and know healthcare related services over internet or mobile networks. In order to obtain this, several smart card based authentication schemes for telecare medicine information systems have been introduced. An improved protocol is used to secure the data. A smartcard can be used to store the data about the patient. The registration phase has been done by including biometric keys. But biometrics can be identified by attacker by using silicone gel. To avoid this weakness, locking system will be proposed. If any attacker accesses the account, the notification will send to the user about the invalid access with locking system and the user can lock the system. So the attacker could not access the account further. Then the user unlocks the account by using the security questions which are given at the registration phase. After that the user can change the password and use the account securely.

V. REFERENCES

[1] Ankita Chaturvedi et al(Dec 2014),"An enhanced dynamic ID-based authentication scheme for telecare medical information systems", Journal of King Saud University – Computer and Information Sciences

[2] Kukki Arya and Abhinav Vidwansh (Jul 2015), " Survey of Authentication Schemes used for Telecare Medicine Information Systems ", International Journal of Computer Science Engineering (IJCSE).

[3] Zuowen Tan (2013)," An efficient biometrics-based authentication scheme for telecare medicine information systems", Jiangxi University of Finance & Economics.

[4] Min Zhang et al (2014),"A Secure Sketch-based Authentication Scheme for Telecare Medicine Information Systems", Southwest JiaoTong University.

[5] Yang sun(2016)," An Improved Password Authentication Scheme for Telecare Medical Information Systems Based on Chaotic Maps with Privacy Protection", Shenyang Normal University

[6] Wenhao Liu et al (May 2016), "An improved authenticated key agreement protocol for telecare medicine information system", a SpringerOpen Journal.

[7] L.P. Zhang et al (2015),"Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme", IEEE Journal of Biomedical and Health Informatics, DOI 10.1109/JBHI.2016.2517146.

[8] Bhundiya Mehul (2016)," Create Notification Alert using Notification Manager in Android", The APPGuruz.

AUTHOR'S BIOGRAPHY

K.Prem Kumar received B.Tech degree in Information Technology from Anna University, Chennai in the year 2010. He received M.E degree in Compueter Science and Engineering in the year 2015 from Anna University, Chennai. Currently He is working as Assistant Professor in Department of Computer science and Engineering at M.Kumarasamy college of Engineering,Karur. His research area is Data security and Data analytics.

P.Gayathri received the B.E degree in Computer Science and Engineering from Anna University, Chennai, TamilNadu, India in 2015. Currently, she is pursuing her Master degree in the area of Computer Science and Engineering in M.Kumarasamy College of Engineering, Karur. Her area of interest is Network Security.