AUTHENTICATION FOR BANKING USING HOMOMORPHIC ON CLOUD

[1]Kalaiarasi G, [2]Subashini V, [3]Arasu S
Student, Dept. of Computer Science, Loyola Institute of Technology, Chennai[1,2.]
Asst. professor, Dept. of Computer Science, Loyola Institute of Technology,Chennai[3].

ABSTRACT— *In day today life security is needed for all sectors like bank, online transaction etc. Smart-card-based password authentication is one of the most commonly used security mechanism. This is used to determine the identity of a client, who must hold a valid smart card and the password to carry out a successful authentication with the server. The authentication is usually integrated with a key establishment protocol by using homomorphic algorithm. The paper is to avoid use of active attack and passive attack. So, we present a single card number which allows to access the bank account.*

Keywords— smartcard, key ,password authentication, dictionary attack.

1, INTRODUCTION

Shopping and online banking occurs constantly in the internet marketplace.Unfortunately online fraud and identify theft occurs just as frequently.Online transaction always carry some risk,butr consumers can do many things to increase their security on the web.Banking is an attractive target for criminal account takeover due to the rapidly growing number of users and limited fraud detection and prevention capabilities.To successfully combat these constant threads,banks and financial institutions need a new paradigm one that provides effective,non intrusive and frictionless banking. A commonly used user identification method relies on profiling as a means of identifying fraudulant transaction.Due to the sastical nature of some approaches false negatives and false positives frequently occur.

Todays malwares includes a variety of attack types.Data-and credential-stealing malware comes in the form of fake applications,SMS stealers and PC/mobile combination malware.Bank websites generally have enhanced"green bar" SSL certificates which makes them reasonably easy to recognise,but there are still lots of other security threats.Most of the PC s can be controlled by hostile software,they all can be deafted by malware that takes over the users web browser,so the user does the process to login.

This model initiates the study of two specific security threads on smart-card-based password authentication in distributed system. Smart-card-based password authentication is one of the most commonly used security mechanism to determine the identity of remote client, who must hold a valid smartcard and the corresponding password to carry out a successful authentication with the server. The authentication is usually integrated with a key establishment protocol and yields a smart-card-based password authentication key agreement. Using two recently proposed protocol as case studies, we demonstrate two new types of adversaries with smart card adversaries with pre computed data stored in the smart card adversaries with different data(with respective different timeslots) stored in the smartcard. These threats, though realistic in distributed system, have never been studied in the literature. In addition to point out the vulnerabilities, we propose the countermeasures to thwart the security threats and secure the protocol. In most smart-card-based password authentication schemes, smart cards only store the data produced during the registration phase. As a result, an adversary with the smart card can only obtain the data generated in that phase.

The objective of this model is to avoid use of active and passive attack(dictionary attacks)

Fig 1.Smartcard based security

2, SYSTEM ANALYSIS

2.1 Existing System

Todate,many smart-card-based password authentication schemes have been proposed,and various security goals and propertirs have been addressed,including(but are not limited to) low computation and communication cost,no password table,security against replay attacks,security against parallel session attacks,mutual authentication,session key aggreement and security against adversaries with smartcard.

It is not trivial to design smart-card-based password authentication satisfying even the basic requirements,and infact many schemes have been found broken shortly after their proposals.A user is allowed to choose his/her password in the password changing phase.It is well a known problem that human memorable passwords only come from a small domain.Which is known as dictionary attack.Dictionary attacks can be further divided in to online(active)and offline(passive)dictionary attack.

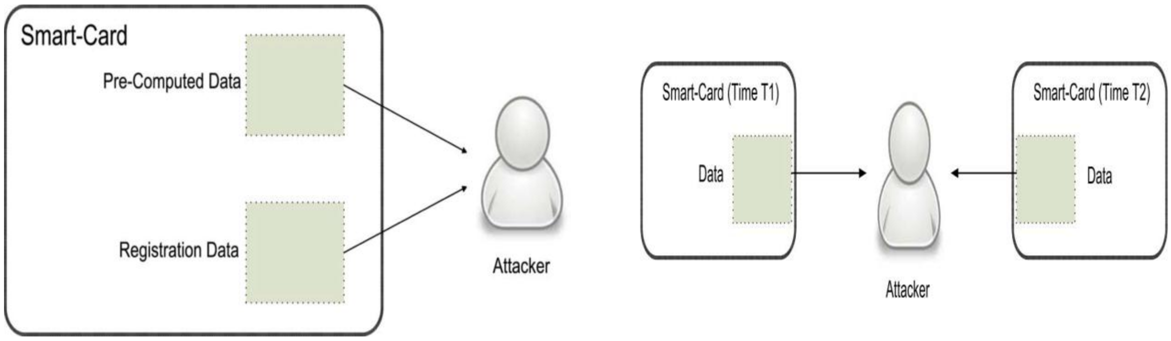
.

3,Adversary models:

An attacker can make successful log-in only with the smart card.Smart-card-based password authentication protocal may be faced with a passive attacker and an active attacker.A passive attacker can obtain messages transmitted between users and the server.An active attacker can also request session keys adaptively.It is evident that an active attacker is more powerful than a passive attacker.There are two types of adversaries.

Fig.3.1.Attacker with Pre-Computed and different

Data In the smart card.



4,PROPOSED SYSTEM:

Recently,two smart-card-based password authentication schemes were proposed which describes a robust and efficient user authentication and key aggreement scheme using smartcard.New adversaries with smartcard that is precomputed data stored in the smart card.We proposed to fix the flaw,together with several new properties such as forward secrecy and password changing without any interaction with the server.The security analysis made indicates that the improved scheme remains secure under offline dictionary attack in the smard card loss case.The scope of the model is to give security for transaction purpose and provide single card number to remember instead of remembering stored in the smart card itself.

4.1,ADVANTAGES:

- Costly operations are completed in the offline phase(before the authentication).
- It is claimed that this scheme can prevent offline dictionary attacks.
- Attacks even if the secret information stored in a smart card is compromised.

5, IMPLEMENTATION:

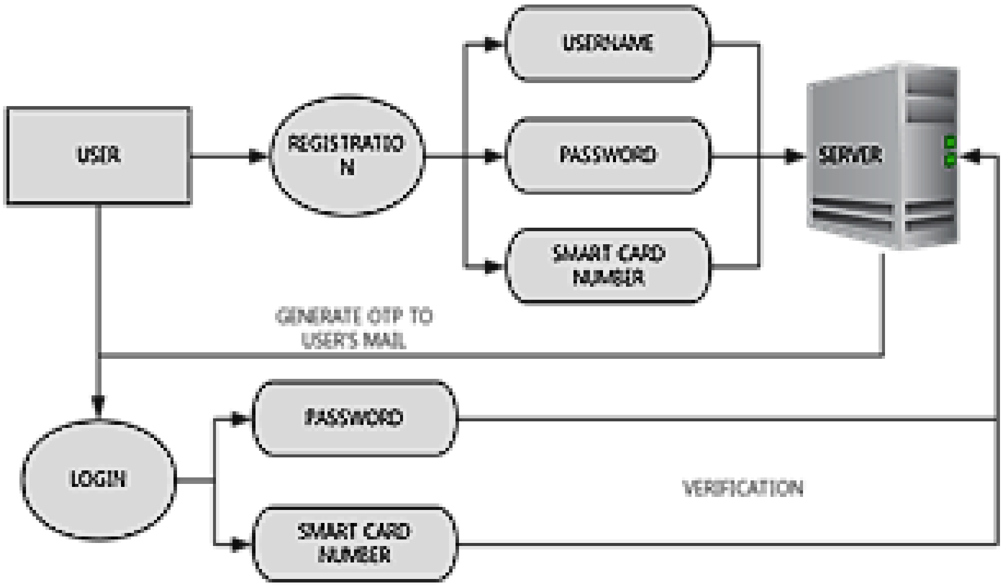


Fig.5.1 System Architecture

5.1,User Authentication:

The user creates the smartcard by providing the recommended details.The user provides the fingerprint as an additional authentication for security.The user access the bank details through username and password,here password act as a dummy password.A smart card based password authentication is used to login for every user.Smartcard validation will happen in the server.

5.2,Session Key Extraction:

The dummy password which has been given in the smart card creation phase acts as a session key.Using the session key,the OTP which is the actual key for encrypting is being generated.Session key is stored in an encrypted form so that attackers cannot get the password.

5.3,Fingerprint Authentication:

It is used as an additional authentication for security purpose.Once the user logins using the dummy password the fingerprint image is required for the further transaction.The fingerprint given here should match with the original finger print which is been given in the card creation phase.Only if this process is completed then the OTP will be generated to the user mail id.

5.4,Current Password Extraction:

Since the fingerprint is being authenticated the OTP will be generated to the user mail id.Using the generated OTP the user encrpts the new password for the further transaction.If the adversary tries to hack the password we will get an alert to the user mail because the AES algorithm has been used for fixed password length.The adversary tries the password with more or lesser than the fixed length,an alert will be generated to the mail.The session out time for the password entry is 30 secs.

5.5,Password Changing Phase:

If the adversary can capture the information in the smart card once,we believe the adversary can also do it for the second time.This is also a reasonable assumption as changing password on a regular basis has been regarded as one of the good password habbit.This completes the description of the attacking scenario we are concerned about which we believe false into the category of passive attacker with smart card defined.So that in this scenario the user gives the new password each time, it becomes a tedious process for the adversaries.

6, CONCULSION AND FUTUREWORK:

Based on several analysis, our system proved to be efficient and user friendly for secured login to perform online transaction.Especially this can resist the offline dictionary attack,based on the user s smart card password authentication scheme.Our result can further help to advance this technology towards practical applications.

REFERENCES

#1 “ Further Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards ” Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo IEEE 2004.

#2 ” Robust Remote Authentication Scheme With Smart Cards “ Chun-I Fan ,Yuang-Cheng Chan , Zhi-Kai Zhang IEEE 2005.

#3 “ A k-Nearest Neighbor Approach for User Authentication Through Biometric Keystroke Dynamics” J.Hu, D.Gingrich, A.Sentose IEEE 2008.

#4 “ Security Weakness of Song s Advanced Smart Card based Password Authentication Protocol ” Wen-Bing Horng,Cheng-Ping Lee, Jing-Wen Peng IEEE 2010.

#5 “ A Robust And Efficient Password-Authenticated Key Agreement Scheme Without Verification Table Based on Elliptic Curve cryptosystem “ Hongfeng Zhu, Tianhua Lua IEEE 2010.

BIOGRAPHY

[1]**Kalaiarasi G** currently pursuing B.E(final year) Computer Science and Engineering in Loyola Institute of Technology.

[2]**Subashini V** currently pursuing B.E(final year) Computer Science and Engineering in Loyola Institute of Technology.

[3]**Mr.S.Arasu** received B.E(CSE) from the V.S.B Engineering College affiliated to Anna University and received M.Tech(CSE) from Bharath University.Currently he is an Assistant Professor in the department of CSE in Loyola Institute of Technology.He published one paper in Journal ,National Conference and International Conference.Total experience as Assistant Professor of around 4 years 10 months.He is a member of ACM.