International Research Journal of Education and Technology

Peer Reviewed Journal

ISSN 2581-7795

Analysis of Extended Security model based on Smart Card using Anonymous Two Factor Authentication Key Exchange Protocol

Sulochana Gamoth, Lokendra singh Songare

PG Scholar, CSED, Dr. APJ Abdul Kalam University Indore, M.P., India

Assistant Professor, CSED, Dr. APJ Abdul Kalam University Indore, M.P., India

ABSTRACT

In this thesis we initiates the analysis of twin specific or particular or especially security threats (means of declaration of an intention or a determination to inflict harm on another) on smart card based password authentication (or authorization processing) in distributed systems. Smart- card-based password authentication is one amongst the foremost usually used security mechanisms to see the identity of a distant consumer, who should hold a legitimate smart card and also the corresponding password to hold out a prospering authentication with the server. Such security is required when there is fear of dictionary attack, in dictionary attack there are some lists of pre-computed words in order to guess the password to access the system. The authentication is typically integrated with a key establishment protocol and yields smart-card- based password-authenticated key agreement. Victimize two recently planned protocols as case studies, we tend to demonstrate two new forms of adversaries with sensible card:

(1) Adversaries with pre-computed information hold on within the smart card, and

(2) Adversaries with totally different or completely different information (with relation to different time slots) hold on within the smart card. These threats, although realistic in distributed systems, haven't been studied within the literature. Additionally to imply the vulnerabilities, we tend to propose the countermeasures to thwart the safety threats and secure the protocols.

Key Words: smart card, authorization processing, security threats, Research Expertise,

INTRODUCTION

In any electronic transaction twat document in the two parties or more than two parties don‟t want to trust each other or each other transactions that are why a type of signing protocol is needed in the situation which is known as a normal language a contract signing protocol. The contract signing is easy in paper based model due to existence of simultaneous. Two parties hard copy of the same contract are approved or signed by the both the parties at the same time and at the same place. After the contract signing both of them are approved on that document. So, if one of them do not agree on that document or contract then the other one is must provide the signed document in the court. Now a day"s many business oriented application or business uses the electronic transactions, for electronic transactions we are using key transfer protocol. When we talk about paper based contract then the signing on that document is very necessary and both the person have sign on that document at the same time and same place. If both the parties are unable to meet for signing on the contract, then the scheme electronic signing contract is the next alternative. When both the parties having lack of trust then this scheme which is known as electronic contract signing is totally fail. Many time one party or one user may send their electronic signature to other party but in many ways the other person or party may not return the signature to other party. For solving this problem, we are using group key establishment scheme. With the help of this scheme we can establish a common session key which is known by only the authorized group member but not other for communication. For this we are using key transfer protocol. In this protocol we are using key generation center (KGC) which is generate session keys for communication.

Before a long time, we were providing authentication with the physical appearance of person and by their signature manually, but now a day"s different techniques were implemented. One of them is contracts signing. Contract signing is very important protocol by which we can exchange our data by online. So with the help of this technique we can prevent different attack so the solution is implemented a new scheme or new protocol which is more efficient and more secure and preventing from different attacks which can be used in a variety of applications especially in E-commerce. This technique allows an efficient signing between two parties such that the chances of attacks reduce. The technique is based on trusted third party so that the

chances of eavesdropping are less. The technique is based on one time where after signing contract between parties the key destroys.

OBJECTIVE OF THE WORK

Here we conclude that the many of them researcher face common problem to design a secure system like smart card. Drawback and problem issues facet by the researcher or previous design algorithm given below.

- Secret information stored in the smart card is compromised
- inability of password changing operation
- attacker uncover password using offline dictionary attack
- Problem in log in phase
- Some security issue
- Offline dictionary attack
- In password changing phase adversary can successfully guess the password
- Online dictionary attacker with the smart card can also discover the password chosen by user in login phase

Problem in authentication phase because they are using only two stage authentication private key and master key only.

PROPOSED WORK

The smart card contains the public parameter IM and a private parameter V. As discussed in here, an adversary cannot directly use $V = h(ID||K_S)\oplus h(PW)$ to corrupt the user U‟‟s authentication session. This is due to the fact that V does not provide any useful information about the password PW, if the server‟s secret key K_S is selected from a large domain. In other words, the information V alone does not help the adversary to verify the guess of a user‟s password. The question arises: With two (or more) Vs generated at different times, whether or not the adversary can uncover the user‟s password?

RESULT: -

In this section we discussed the results related to our proposed methodology. We are using Net-Beans IDE 8.1 as a simulation tool. NetBeans is an integrated development environment for developing primarily with Java, but also with other languages, in particular PHP, C/C++, and HTML5. It is also an application platform framework for Java desktop applications and others. The NetBeans IDE is written in Java and can run on Windows OS.

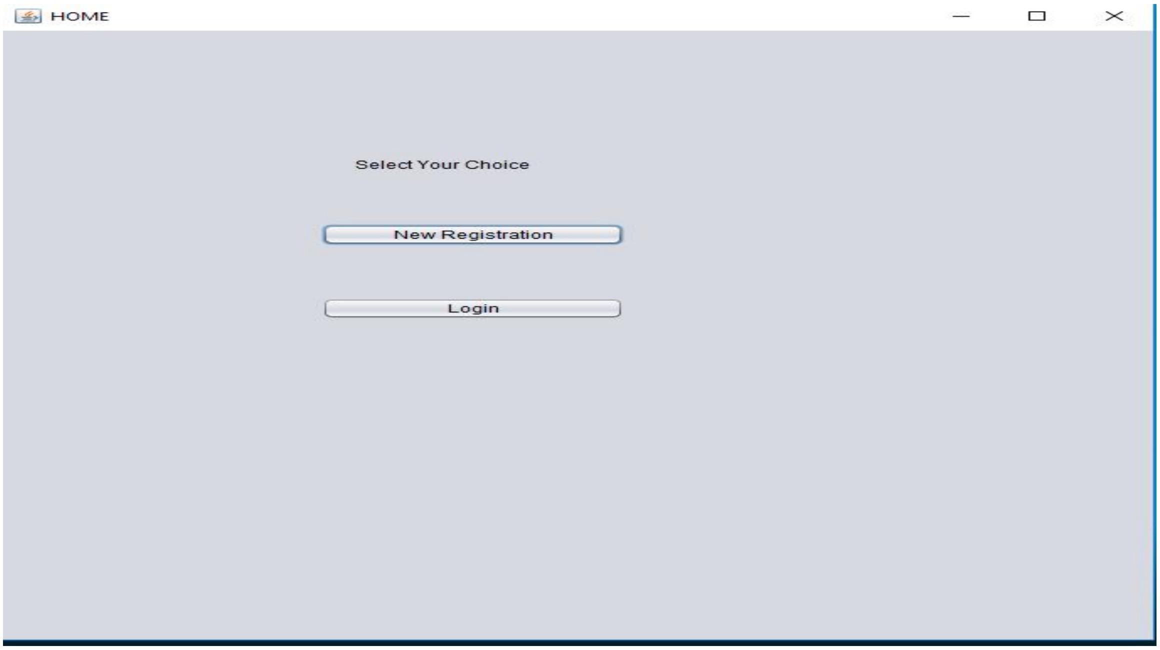
The NetBeans Platform is a reusable framework for simplifying the development of Java Swing desktop applications. The NetBeans IDE bundle for Java SE contains what is needed to start developing NetBeans plug-in and NetBeans Platform based applications; no additional SDK is required. Applications can install modules dynamically. Any application can include the Update Centre module to allow users of the application to download digitally-signed upgrades and new features directly into the running application. Reinstalling an upgrade or a new release does not force users to download the entire application again.

The platform offers reusable services common to desktop applications, allowing developers to focus on the logic specific to their application. Among the features of the platform are

1) User interface management e.g. menus and toolbars
2) User settings management
3) Storage management or saving and loading any kind of data
4) Window management
5) Wizard framework (supports step-by-step dialogs)
6) NetBeans Visual Library
7) VII Integrated Development Tools

SIMULATION RESULTS

Simulation of our proposed methodology perform on the simulation software Net-Beans IDE 8.1. In this section we discussed the result of two password authentication based smart card model, basically this model consists several modified or improve section related to security analysis like registration phase, Login phase, password changing phase and most importantly the computational complexity as timing, hash function and different encryption functions.



…

Figure 2 Shows that the Main Window of Registration and Login Phase

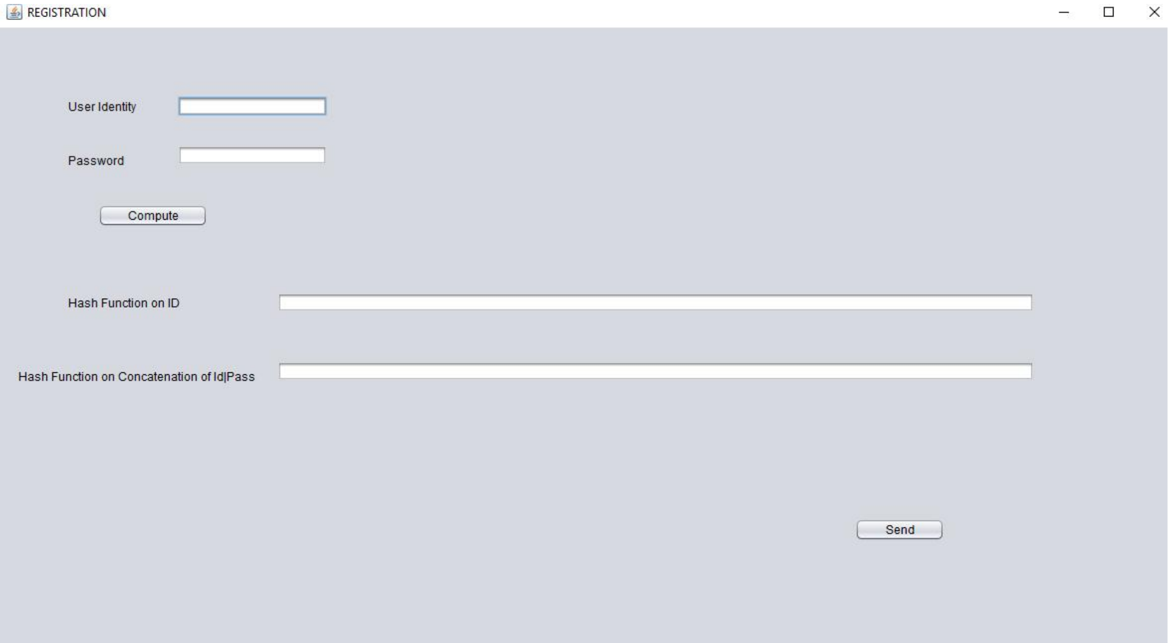
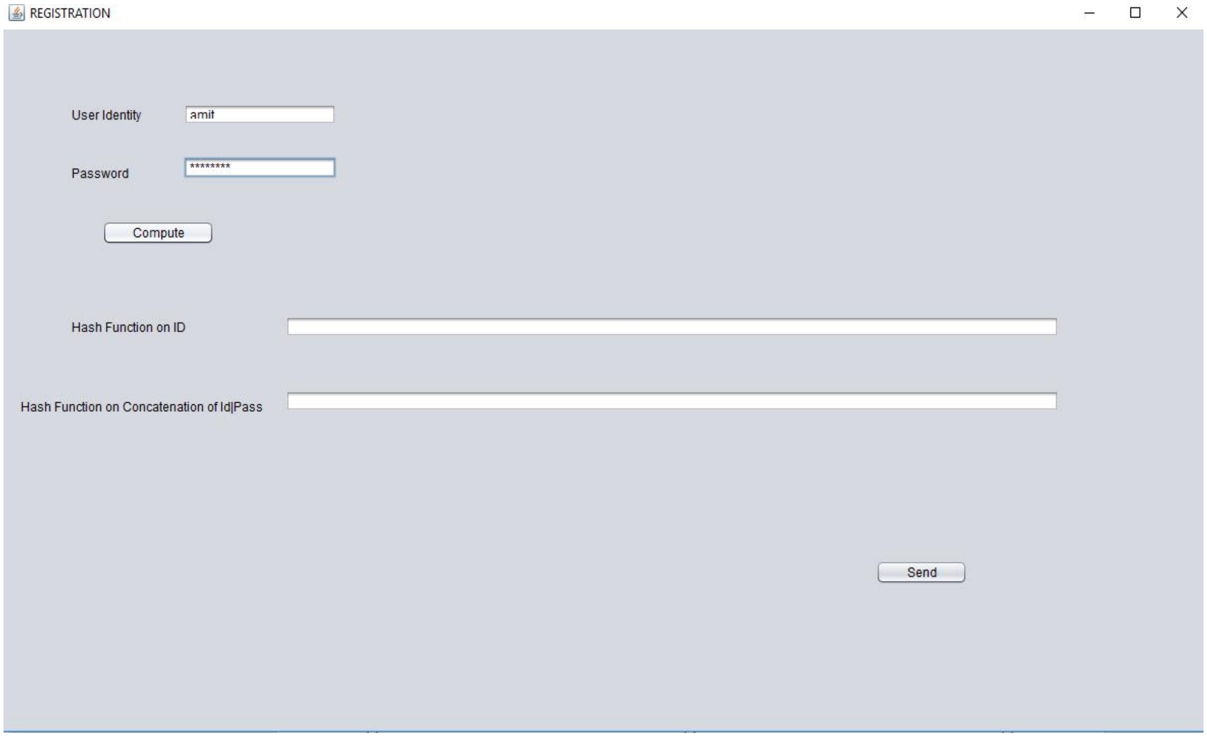


Figure 3 Shows that the Window of Creation of Unique User Identity and Their Password



REGISTRATION

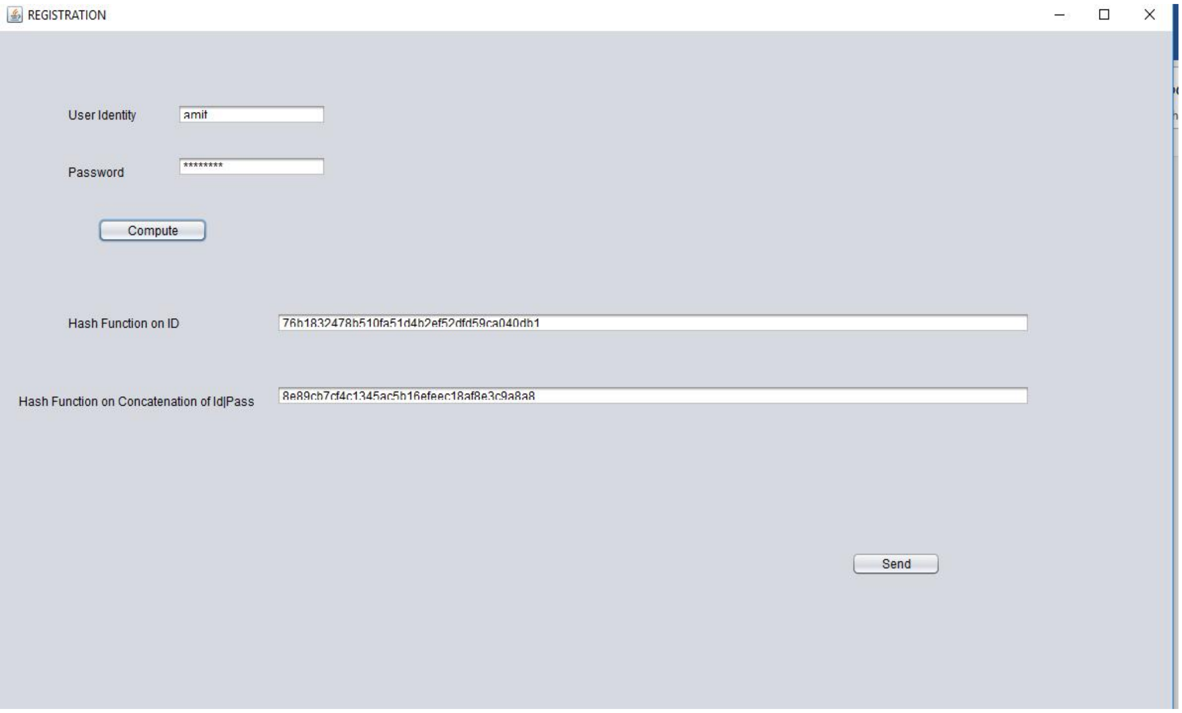
User Identity: amit

Password: ********

Hash Function on ID:

Hash Function on Concatenation of Id|Pass:

Figure 4 shows that for Creation of User ID and Password



REGISTRATION

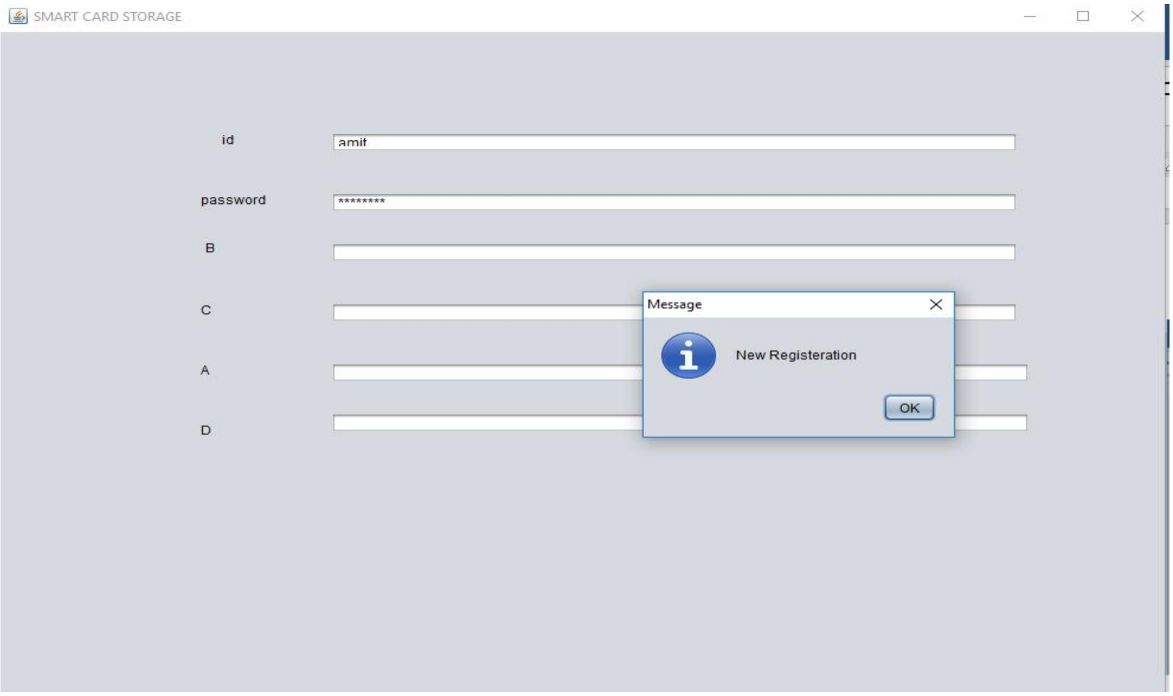
User Identity: amit

Password: ********

Hash Function on ID: 76b1832478b510fa51d4b2ef52dfd59ca040db1

Hash Function on Concatenation of Id|Pass: 8e89cb7cf4c1345ac5b16efeec18af8e3c9a8a8

Figure 5 Shows that the Computation of Hash Function on ID and their Combining Process



SMART CARD STORAGE

id amit

password ********

B

C

A

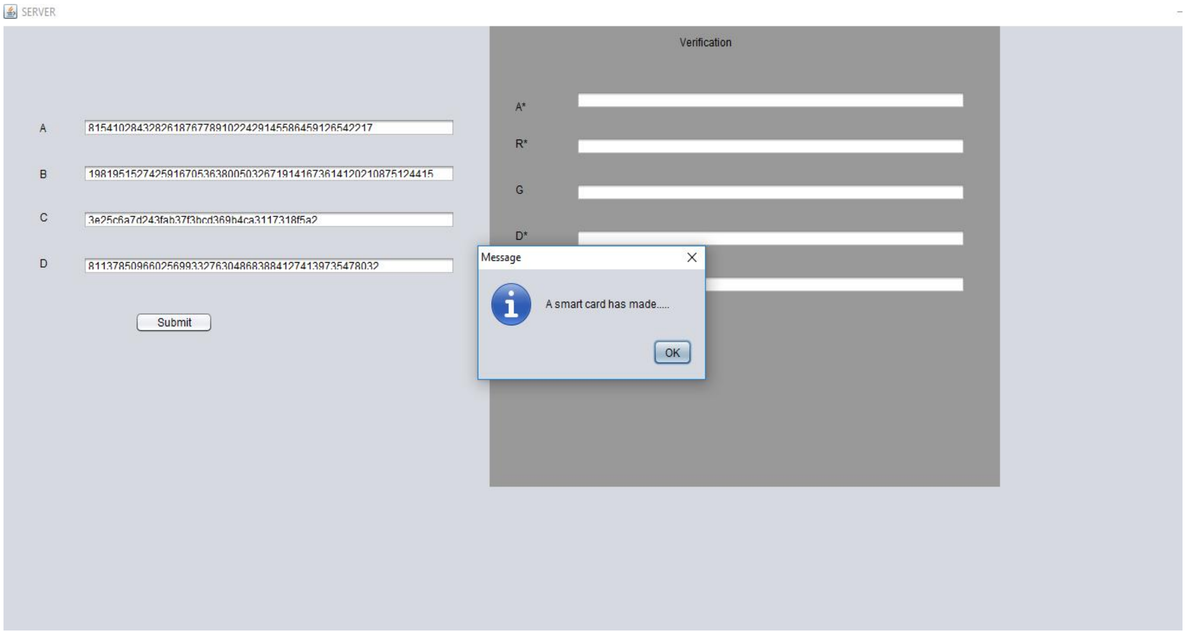
D

Message

New Registeration

OK

Figure 6 Shows that the Confirmation of the New Registration by the Server



SERVER

A 815410284328261876778910224291455864591265422l7

B 198195152742591670536380050326719141673614120210875124415

C 3e25c6a7d243fab37f3bcd369b4ca3117318f5a2

D 811378509660256993327630486838841274139735478032

Submit

Verification

A*

R*

G

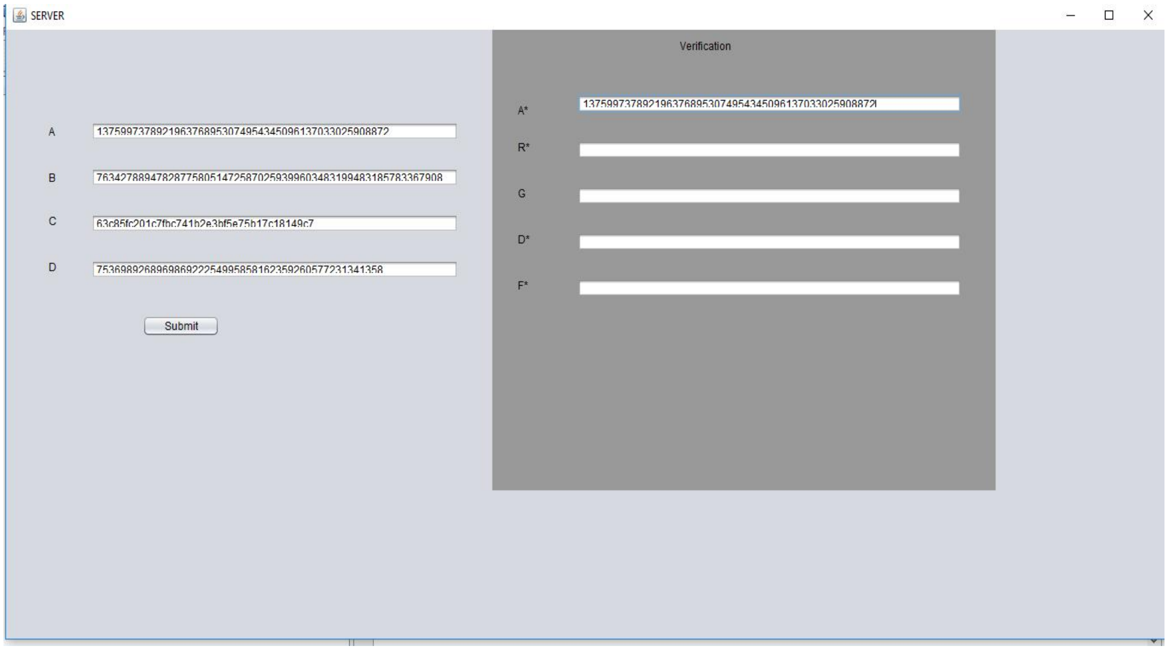
D*

Message

A smart card has made.....

OK

Figure 7 Shows that the message of a smart card has made by Servere Shows that Registered User Computational process



A 1375997378921963768953074954345096137033025908872

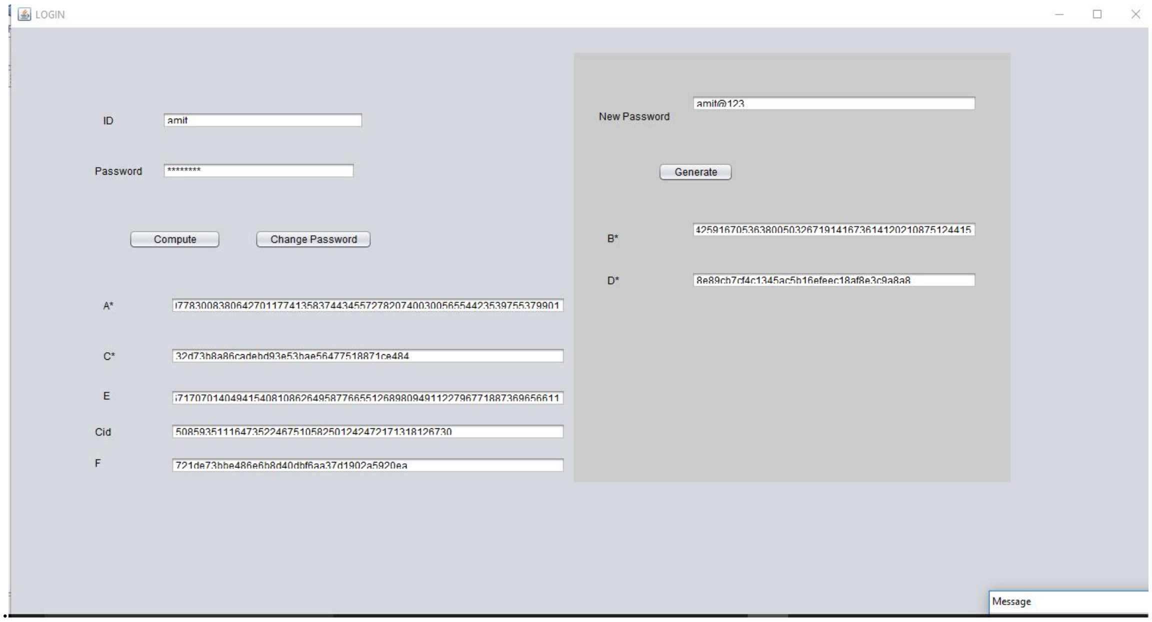
B 7634278894782877580514725870259399603483199483185783367908

C 63c85fc201c7fbc741b2e3bf5e75b17c18149c7

D 753698926896986922254995858162359260577231341358

A* 1375997378921963768953074954345096137033025908872

Figure 8 Shows that Registered User enter Detail Verification process by server



ID amit

Password ********

A* 77830083806427011774135837443455727820740030056554423539755379901

C* 32d73b8a86cadebd93e53bae56477518871ce484

E 71707014049415408108626495877665512689809491122796771887369656611

Cid 50859351116473522467510582501242472171318126730

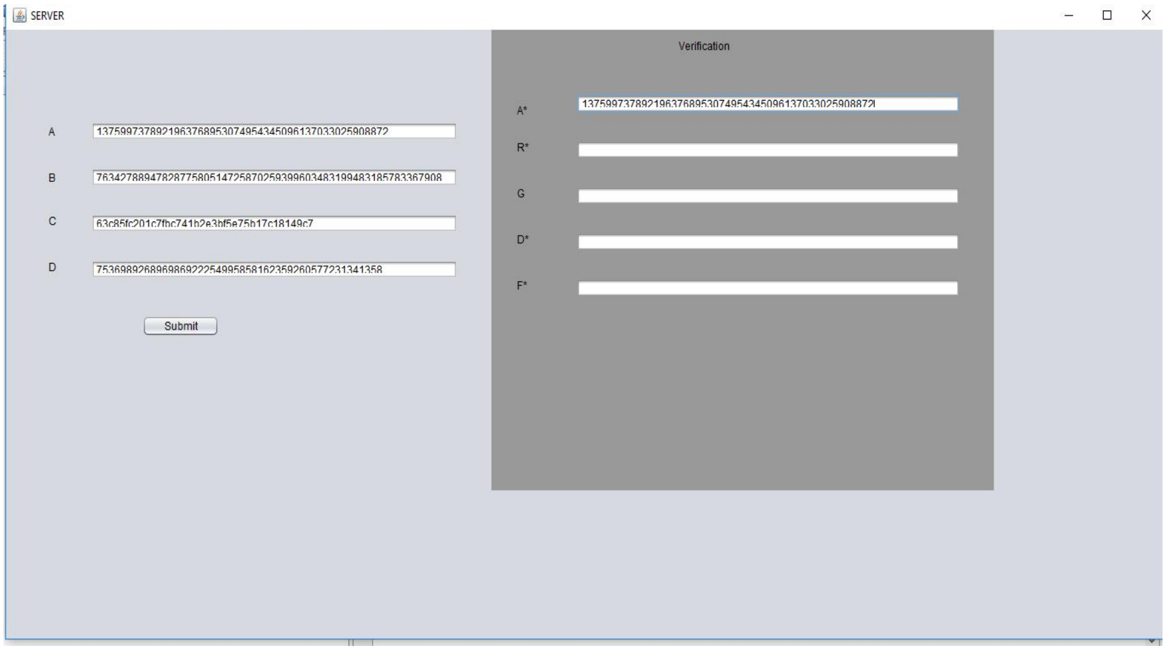
F 721de73bbe486e6b8d40dbf6aa37d1902a5920ea

New Password amit@123

B* 42591670536380050326719141673614120210875124415

D* 8e89cb7cf4c1345ac5b16efeec18af8e3c9a8a8

Figure 9 shows that compution process according to new password



A 1375997378921963768953074954345096137033025908872

B 7634278894782877580514725870259399603483199483185783367908

C 63c85fc201c7fbc741b2e3bf5e75b17c18149c7

D 75369892689698692225499585816235926057723134135 8

A* 1375997378921963768953074954345096137033025908872

R*

G

D*

F*

Figure 10 shows that Registered User enter Detail Verification process by server

.slogin with user id and new password which had changed currently. Figure Shows that it confirmed that user enter correct user id and password or not.it verifies on the basis of matching the hash key stored on the smart card storage and computed hash key at the time of login. Figure
that it computes other computation keys according to current user id and password. Figure 5.24 Shows that Login user detail verified by the server,it verified according to login user details which information also stored on server,server match both detail if match then it verifies to user. Figure 5.25 Shows that after verified login user by server.server create or generate session key by server of login user. Figure 5.26 Shows that after create session key login user confirmed by the server so that user can perform the transaction.

EXPERIMENTAL RESULT ANALYSIS

Attack	**Existing Scheme(attack prevention)**	**Our Scheme(attack prevention)**
Replay attack	**No**	**Yes**
Identity disclosure attack	**No**	**Yes**
Insider attack	**Yes**	**Yes**
Outsider attack	**No**	**Yes**
Eavesdropping	**No**	**Yes**
Identity Spoofing	**Yes**	**Yes**
Password based attack	**No**	**Yes**
Man-in the middle attack	**No**	**Yes**

Table 1 Prevention from Various Attacks

No. of bits in token	No. of bits in conceal value	Time taken
32	128	12.540 sec

Table 2 Time taken and No. of bit used

Storage/ scheme	Existing Work	Our scheme
Smart card	128 bits	256 bits
Server	64 bits	128 bits

Table 3 Storage judgment of the planned scheme

Computation Cost		Existing Scheme	Our Scheme
Smart Card	Registration Operation	-	-
	Session Run	2M+4H	1M+2H
	Password Operation	2H	1H
Server	Registration Operation	2H+1E	1H+1E
	Session Run	2M+4H+1E	1M+2H+1E
	Password Operation	-	-

Table 4 Comparison of Computation with previous work

Where, H denotes the cryptographic hash computation & M denotes the scalar multiplication computation over the elliptic curve & E denotes the symmetric encryption or decryption computation. These above table are the Comparisons table with Previous work.

Conclusion-

This dissertation revisited the security of two password authenticated key agreement protocols using smart cards. While they were assumed to be secure, we showed that these protocols are flawed under their own assumptions respectively. In particular, we took into account some kinds of adversaries which were not considered in their designs or methodology, e.g., adversaries with pre-computed data stored like (registration information, and other related information of account and user identification) in the smart-card and adversaries with different data (with respect to different time slots) stored in the smartcard.

These adversaries represent the potential threats (means of declaration of an intention or a determination to inflict harm on another) in distributed systems and are different from the commonly known ones, which we believe deserve the attention from both the academia and the industry.

We also implement or designed the solutions to fix these security flaws. So we have done several analysis during this dissertation, simulation results of our proposed methodology of password based smart card authentication has highlight the importance of elaborate or brief analysis the security models and formal security analysis on the design of password- authenticated key agreement protocols using smart cards. Simulation results shows that we have using less number of hash function and elliptical function to design this system. We have focused only the how to be combining the operation of registration and login section (i.e. user ID with password) with fewer hash function and their combining. The main aim of this dissertation is reduce the complexity and cost of the system and this aim achieved by implement this proposed improvement of password authentication based smart card scheme. From the results table we can see that these improvements in term of time complexity and size and cost.

REFERENCES

[1] Alfin Abraham, Vinodh Ewards, Harlay Maria Mathew "A Survey on Optimistic Fair Digital Signature Exchange Protocols", International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, Vol. 3, No. 2, pp. 821 – 825, Feb 2011.

[2] Qi Xie, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming Fang," Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model", IEEE Transaction 2016.

[3] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transaction 2016.

[4] C. Boyd, "On Key Agreement and Conference Key Agreement," Proc. Second Australasian Conf. Information Security and Privacy (ACISP "97), pp. 294-302, 1997.

[5] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information

Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[6] Vinod Moreshwar Vaze," Digital Signature on-line, One Time Private Key [OTPK]", International Journal of Scientific& Engineering Research Volume 3, Issue 3, March -2012 1 ISSN22295518".

[7] H. Pagnia, H. Vogt and F. C. Gartner," Fair Exchange" The Computer Journal, 2003.

[8] R. Madhusudhan and Manjunath Hegde, "Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card", IEEE 2016.

[9] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, and Li Xu, "Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems", IEEE Transaction 2014.

[10] ZHANG Gefei, FAN Dan, ZHANG Yuqing and LI Xiaowei, "A Provably Secure General Construction for Key Exchange Protocols Using Smart Card and Password", Chinese Journal of Electronics 2017.

[11] Zheng xian Gao, Shou Hsuan Stephen Huang, Wei Ding, "Cryptanalysis of Three Dynamic ID-Based Remote User Authentication Schemes Using Smart Cards", IEEE 2016.

[12] S. Micali, "Simple and fast optimistic protocols for fair electronic exchange," in Proc. PODC"03, 2003, pp. 12–19, ACMPress.

[13] G. Wang, “Generic non-repudiation protocols supporting transparent off-line TTP,” Journal of Computer Security, vol. 14, no. 5, pp. 441–467, Nov. 2006.

[14] Vinod Moreshwar Vaze,” Digital Signature on-line, One Time Private Key [OTPK]”, International Journal of Scientific & Engineering Research, ISSN:2229-5518, Volume 3, Issue 3, March -2012.

[15] Lein Harn a,Chu-Hsing Lin “Contract signature in e-commerce”, Computers and Electrical Engineering vol.-37, pp-169–173, 2011.

[16] Alptekin Kupcu and Anna Lysyanskaya, “Optimistic Fair Exchange with Multiple Arbiters”, Brown University, Providence, RI, USA, 2008.

[17] H.Jayasree1 and Dr. A.Damodaram “A Novel Fair Anonymous Contract Signing Protocol for E-Commerce Applications” 2012 International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.

[18] Ying Zhang, Chenyi Zhang, Jun Pang and Sjouke Mauw “Game-Based Verification of Multi-Party Contract Signing Protocols”, Formal Aspects in Security and Trust, Lecture Notes in Computer Science, Volume 5983, pp 186-200, 2010.

[19] Mihhail Aizatulin, Henning Schnoor, and Thomas Wilke “Computationally Sound Analysis of a Probabilistic Contract Signing Protocol”, Computer Security – ESORICS 2009, Lecture Notes in Computer Science, Volume 5789, pp. 571 - 586, and 2009.

[20] Debajyoti Konar and Chandan Mazumdar “A Novel Fair GSR Contract Signing Protocol against Earnest Money” International Journal of Computer Science and Network Security (IJCSNS), VOL. 7, No. 11, November 2007.

[21] Jose A. Onieva1, Jianying Zhou, and Javier Lopez “Analysis of an Asynchronous Multi Party Contract Signing Protocol”, Progress in Cryptology - INDOCRYPT 2005, Lecture Notes in Computer Science, Volume 3797, pp 311-321, and 2005.

[22] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 591–606, Apr.2000.

Guilin Wang. “An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature”, IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1, March 2010..