International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

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

Amit Manjhi[1], Pradeep Kumar Mishra[2], Saurabh Jain[3]
[1]M.Tech Scholar, [2]Assistant Professor, [3]Assistant Professor, Department of Computer Science Engineering, OCT, Bhopal, India

Abstract- **In this paper we initiate 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. 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: Adversaries with pre-computed information hold on within the smart card, and 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.**

Keywords: **Smart Card, Random Key Generation, Two-PAKE, Online Dictionary Attack, Offline Dictionary Attack, Session Key, Authentication and Authorization.**

I. 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 no 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.

Long time ago, 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.

Proper security is achieved if exchange protocol having no los-preventing property. Loss preventing property means any party incurred no loss at all with other party. We can say that this protocol provides true fairness whenever parties exchange their data or information to each other or not.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

The protocol itself is relatively simple find computationally efficient. For secure communication we can maintain Third Trusted Party which always be online which is more expensive. Now TTP which was used as online .it become offline and we can easily maintain offline TTP, which also provide secure exchange of information [1]. This protocol is not practical for large amount of communication involved. In authorized exchange protocol with an online TTP, a TTP must be involved in all exchange and it must be presence in entire communication. This protocol is very simple and computationally efficient. But maintain on line TTP is very costly and expensive.

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card that has embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate. Since April 2009, a Japanese company has manufactured reusable financial smart cards made from paper.

Smart cards can be either contact or contactless smart card. Smart cards can provide personal identification, authentication, data storage, and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations.

Design of Smart Card

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimeters (3.37 in × 2.13 in). Another popular size is ID-000 which is nominally 25 by 15 millimeters (0.98 in × 0.59 in) (commonly used in SIM cards). Both are 0.76 millimeters (0.030 in) thick.
- Contains a tamper-resistant security system (for example a secure crypto-processor and a secure file system) and provides security services (e.g., protects in-memory information).
- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.
- Communicates with external services via card-reading devices, such as ticket readers, ATMs, DIP reader, etc.

There are four types of smart card and these are as follows:

1. Contact Smart Card
2. Contact-less Smart Card
3. Hybrid
4. USB

II. Related Works

In this section we present the conclusion results of existing Authentication techniques for network security or security providing in data sharing. Password authentication based smart card technique in a very popular and computationally expensive task.

The paper [2] proposed an Anonymous Two-Factor AKE scheme which preserves security against various attacks including de-synchronization attack, lost-smart-card attack and password guessing attack, and supports several desirable properties including perfect forward secrecy, anonymity or un-traceability, adaptively password change, no centralized password storage, and no long-term public key. Furthermore, our protocol maintains high efficiency in terms of storage requirement, communication cost as well as computational complexity. Our protocol requires only a few number of message flows and all the transmitted messages are short in size. Additional, the proposed scheme is provably secure in our extended security model of AKE. Therefore, the proposed scheme is suitable for deployment in various low-power networks, in particular, the pervasive and mobile computing networks.

The paper [3] presented with the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

To overcome this problem, they proposed a shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Furthermore, they implemented a Pass Matrix prototype on Android and carried out user experiments to evaluate the memorability and usability. The experimental result showed that users can log into the system with an average of 1.64 tries (Median=1), and the Total Accuracy of all login trials is 93.33% even two weeks after registration. The total time consumed to log into Pass Matrix with an average of 3.2 pass-images is between 31.31 and 37.11 seconds and is considered acceptable by 83.33% of participants in our user study. Based on the experimental results and survey data, Pass Matrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks. In addition, Pass Matrix can be applied to any authentication scenario and device with simple input and output capabilities. The survey data in the user study also showed that Pass Matrix is practical in the real world.

The paper [4] they presented the cryptanalysis of Wen and Lis an improved dynamic ID based remote user authentication scheme with key agreement, and identified its vulnerability. To overcome the security problems, we proposed improved scheme. Through security analysis, we have explained that, our scheme gives protection from all pointed weaknesses. By performance analysis, we compare the computation cost of our scheme with Wen and Li's scheme and illustrated that our scheme reduces 6 hash function, than their scheme. Hence our scheme is more efficient, particularly for user privacy, amplified security and low computation capability.

This paper [5] 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 types of adversaries which were not considered in their designs, e.g., adversaries with pre-computed data stored 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 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 proposed the solutions to fix the security flaws. Once again, our results highlight the importance of elaborate security models and formal security analysis on the design of password-authenticated key agreement protocols using smart cards.

They propose [6] a general construction for KE protocols using smart card and password. The KE protocols generated from our construction can be used in various public key environments as a basic module.

This new construction also satisfies the AKE security mentioned by Bellare, so that it can resist several attacks including off-line dictionary attack, while many other protocols can't. Applying our construction to the Diffie-Hellman integrated encryption scheme (DHIES) mentioned by M. Abdalla *et al.*, a KE protocol can be obtained, which has not only better security properties, but also better computational efficiency in storage cost and operation time.

III. Proposed Methodology

In the Proposed methodology improved the security at every Phases like registration Phase, Login Phase, Password changing phase and Session Key Generation phase. NETBEANS IDE 8.1used as simulation tool to develop the all the phase and provide Security. In the existing work there are many attack which can successfully Uncover the password chosen by the user offline-dictionary attack and online dictionary attack.

Security Analysis and Improvement

This section describes two types of attacks on proposed scheme, both of which can successfully uncover the password chosen by the user.

A. Offline-Dictionary attacks with Smart Cards

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?

Attacking Scenario.

In this section, we address the attacking scenario as follows.

1) At time T_1, the user invokes the password changing phase to change the password to PW_1.
2) At the end of this phase, the smart card contains (V_1, IM) where $V1 = h(ID||K_S) \oplus h(PW_1)$. At some time later (say, T_2), the user changes the password $PW_1$to a new password PW_2, and the smart card contains (V_2, IM), where $V2 = h(ID||K_S) \oplus h(PW_2)$. PW_2 can be regarded as the current password.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

3) A passive attacker with smart card (defined in Section 3.1) can obtain the data in the smart card at time T_1 and T_2.

We note that such an adversary is stronger than that considered here, where the adversary can obtain the information in the smart card but only once. If the adversary can capture the information in the smart card once, we believe the adversary can also do it for the second time. As an example, one can obtain the information in the smart card via an illegal card reader. This could occur more than once without the awareness of the smart card owner (e.g., the attacker could steal the smart card and send it back after extracting the data stored in the smart card). In the above attacking scenario, the other assumption is that the user will change the password at least twice? We believe this is also a reasonable assumption as changing password on a regular basis has been regarded as one of good password habits.

This completes the description of the attacking scenario we are concerned about, which we believe falls into the category of passive attacker with smart card defined in Section 3.1. It remains to show how to extract the two passwords (PW_1, PW_2) with (V_1, V_2).

how does the attack work?

(V_1, V_2), the adversary can XOR V_1 and V_2 to obtain the equation

$$V_1 \oplus V_2 = h(PW_1) \oplus h(PW_2).$$

This enables the adversary to verify the guess of PW_1 and PW_2, where PW_1 is an old password at time T_1 and PW_2 is the current password at time T_2.

Success Probability.

We now consider the success probability that an adversary can find (PW_1, PW_2) in the above attacking scenario. We will show that the success probability (in general) is at least $1 - \frac{SIZE_{PW}}{SIZE_h}$, where $SIZE_{PW}$ is the size of the password dictionary and $SIZE_h$ is the size of the output domain of the hash function h. In a concrete case, the adversary can find (PW_1, PW_2) with probability almost 1. The detail of our analysis is given as below.

1) By testing all password pairs in the password dictionary, the adversary will find at least one pair (pw_1, pw_2) such that

$$V_1 \oplus V_2 = h(pw_1) \oplus h(pw_2). \quad (1)$$

2) If there is only one pair satisfying Equation. (1), it must be (PW_1, PW_2) and the adversary thus successfully finds the user's passwords.

3) The adversary, however, could find two or more password pairs using Equation. (1). We now consider the probability that there is only one pair satisfying Equation. (1) in the password dictionary.

4) For any two different passwords pw_1 and pw_2 in the password dictionary, we define

$$\mathcal{E}_1: \{pw_1, pw_2\} \neq \{PW_1, PW_2\} \text{ and}$$
$$\mathcal{E}_2: h(pw_1) \oplus h(pw_2) \neq V_1 \oplus V_2.$$

Then, $P_r[\mathcal{E}_1|\mathcal{E}_2]$ is the probability that there is only one pair (PW_1, PW_2) satisfying Equation. (1), i.e., $P_r[\mathcal{E}_1|\mathcal{E}_2]$ is the adversary's success probability to find (PW_1, PW_2).

5) Let $SIZE_{PW}$ be the size of the password dictionary, and let $SIZE_h$ be the size of the output domain of the hash function h.

6) In the password dictionary,

a) For any password $pw_1 \in \{PW_1, PW_2\}$, the probability that there is another password pw_2 such that $h(pw_2) = V1 \oplus V2 \oplus h(pw_1)$ is at most $SIZE_{PW}/SIZE_h$ (assuming the output of h is uniformly distributed). Therefore, for any password $pw_1 \in \{PW_1, PW_2\}$,

$Pr[\mathcal{E}_2| \mathcal{E}_1] \geq 1 - SIZE_{PW}/SIZE_h$.

b) Otherwise, $pw_1 \in \{PW_1, PW_2\}$ but $pw_2 \in \{PW_1, PW_2\}$ (since pw_1 and pw_2 are two different passwords, and $\{pw_1, pw_2\} \neq \{PW_1, PW_2\}$). We first suppose $pw_1 = PW_1$.

In this case, the probability that there is another password $pw_2 \in \{PW_1, PW_2\}$ such that $h(pw_2) = V_1 \oplus V_2 \oplus h(pw_1) = H(PW_2)$ is at most $SIZE_{PW}/SIZE_h$ (assuming the output of h is uniformly distributed). Similarly, for the other case when $pw_1 = PW_2$, the probability that there is another password $pw_2 \in \{PW_1, PW_2\}$ such that $h(pw_2) = V_1 \oplus V_2 \oplus h(pw_1) = H(PW_1)$ is at most $SIZE_{PW}/SIZE_h$ (assuming the output of h is uniformly distributed). Therefore, for any password $pw_1 \in \{PW_1, PW_2\}$,

$Pr[\mathcal{E}_2|\mathcal{E}_1] \geq 1 - SIZE_{PW}/SIZE_h$.

Thus, in either case,

$$Pr[\mathcal{E}_2|\mathcal{E}_1] \geq 1 - \frac{SIZE_{PW}}{SIZE_h}$$

7) We now consider a concrete case. Let the password dictionary consists of 8-character passwords of digits and mixed-case letters, and the hash function h is SHA-256. In this case, $SIZE_{PW}=62^8=218340105584896$, $SIZE_h=2^{256}=1157920892373161954235709850086879078532699846656405640394575840079131296399360$, and $1 - \frac{SIZE_{PW}}{SIZE_h} \approx 1$.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

In other words, the adversary can find the passwords (PW_1, PW_2) with probability almost 1 in this case.

This completes the analysis of Sun et al.'s scheme under a passive attacker with smart card. We have shown that such an adversary can successfully uncover the passwords chosen by the user with overwhelming probability.

B. Online-Dictionary attacks with Smart Cards

An adversary with the Smartcard = {IM, V} can also break the protocol in via an online-dictionary attack. We first outline the active attacker with smart card and then provide the detail description.

The adversary first extracts {IM, V} in the smart card. Then, the adversary inserts the card in the card reader and sends a log-in request on behalf of the user (by inputting a randomly chosen password in a password dictionary). After that, the adversary can uncover the user's password using the response from the server. As in offline-dictionary attacks, we assume again that the user's password is chosen by him/her via the password change phase, rather than the initial one selected by the server. In other words, the password is chosen from a human-memorable domain. The detail of the attack is given below.

Online-Dictionary Attack

1) The adversary first chooses a random number r_C from the interval [1, n − 1], and calculates GC = $r_c \times G$.
2) The adversary sends (IM, G_c) to the Server. Here, IM is stored in the
Smartcard = {IM, V}.
3) The decryption of IM will be correct, and the server will respond with {M_s, G_s}, where
$G_S = r_s \times G$, r_s is randomly chosen in [1, n − 1], $M_S = h_2(K_{su} ||G_c || G_s)$, and
$K_{SU} = h_1(h (ID||K_S)||(r_s \times G_C))$.
4) Upon receiving {M_S, G_S}, the adversary chooses a password pw in the password dictionary and calculates V `= V ⊕ h(pw), K`= h_1 (V||$r_c \times G_s$).
(3. In this case, the adversary (most likely) will not log in successfully, but only one failed log-in attempt will not lead to the lock out of user's account.)
Recall that V is stored in the smart card as well.
5) If the guess of the password is correct, then $M_s = h_2(K ||G_c||G_s)$.
Otherwise, the adversary repeats the calculation at Step. 4 with another password in the dictionary.
6) There is only one correct password in the dictionary, assuming the hash function is collision resistant.
7) The adversary, with the correct password, can either proceed with the remaining steps in the authentication phase or invoke the password-change phase. This completes the analysis of Sun et al.'s scheme under online-dictionary attacks with the smart card. We have shown that an active attacker with smart card can successfully find the user's password using the response from the server. Note that the attacker described above does not log on the server by trying every possible password for a specific user, and is different from the common online-dictionary attacker. More precisely, the adversary described above mounts online-dictionary attacks in a more active way.

IV. Result Analysis

In this section of paper discuss the outcomes of our proposed mechanism for system which are protected from both attacks i.e. online dictionary attack and offline dictionary attack. That security analysis done with the help of Net-Beans graphical user interface. On this platform shows the all the phase which have used in our system propose two factor password authentication based smart card system.

A. Registration Phase:

In Registration Phase Registrant User enter unique Id and Password chosen by user and server successfully encrypt by using hash function, multiplication and cryptographic function. server store the encrypted Id and password and other relevant data and smart card also stored same data. Smart card data which is impossible to decrypt by the attacker.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

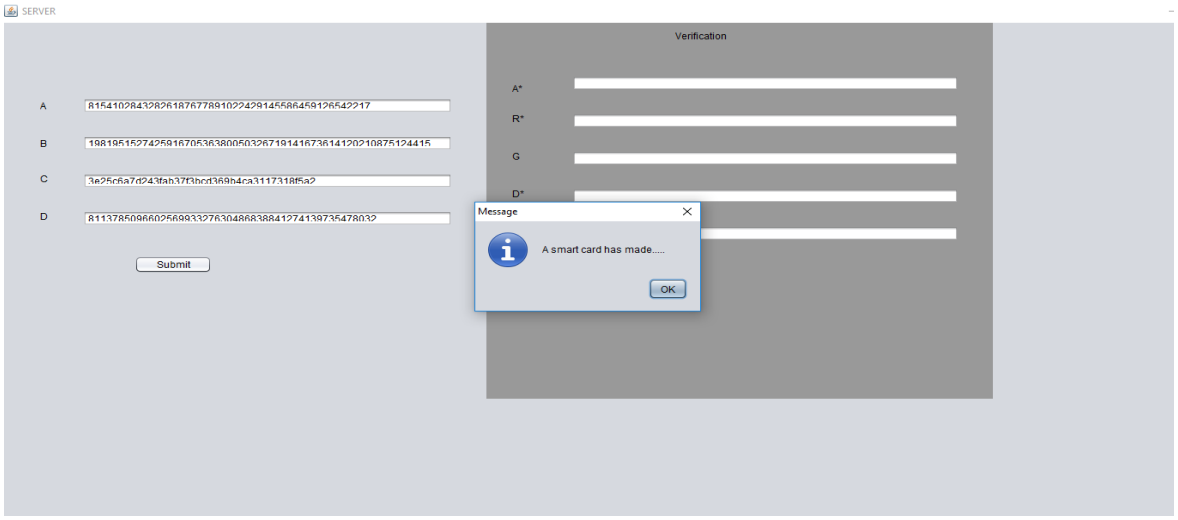

Figure 1. Shows that the message of a smart card has made by Server

B. Login Phase

In login phase only registered user can login which have a valid smart card.

If user want to login, then user have to insert valid smart card and then user have to enter valid user id and password.

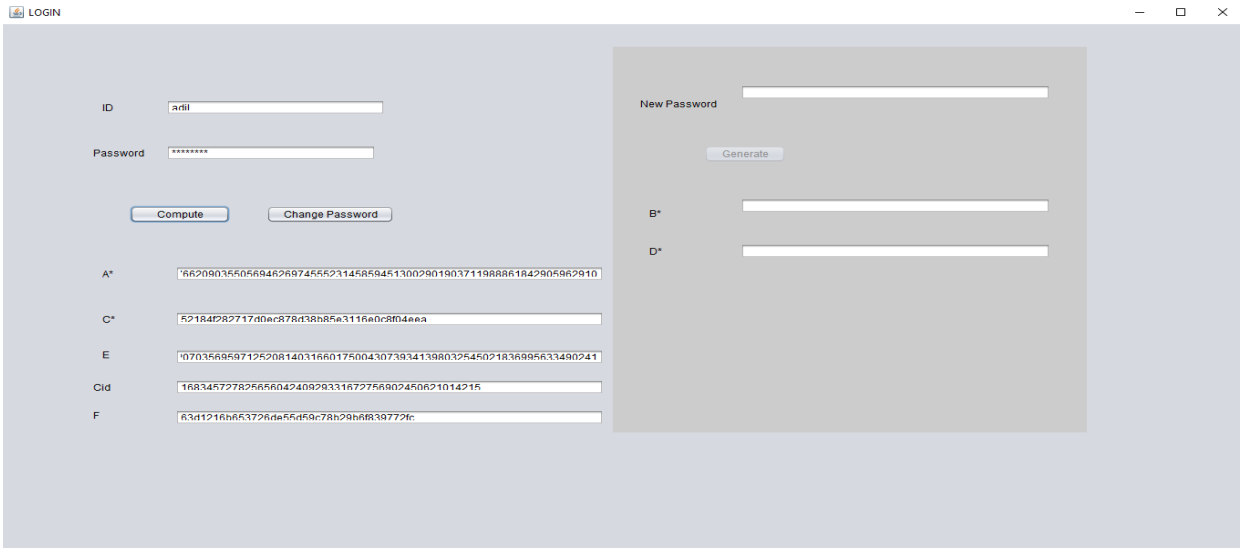

Figure 2. Shows that Registered User Computational process

C. Password Change Phase

In password change phase only registered user can change password which have a valid smart card.

If user want to change password, then user have to insert valid smart card and then user have to access the password change option and then in this phase enter new password and server generate the encrypted key according to new password.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

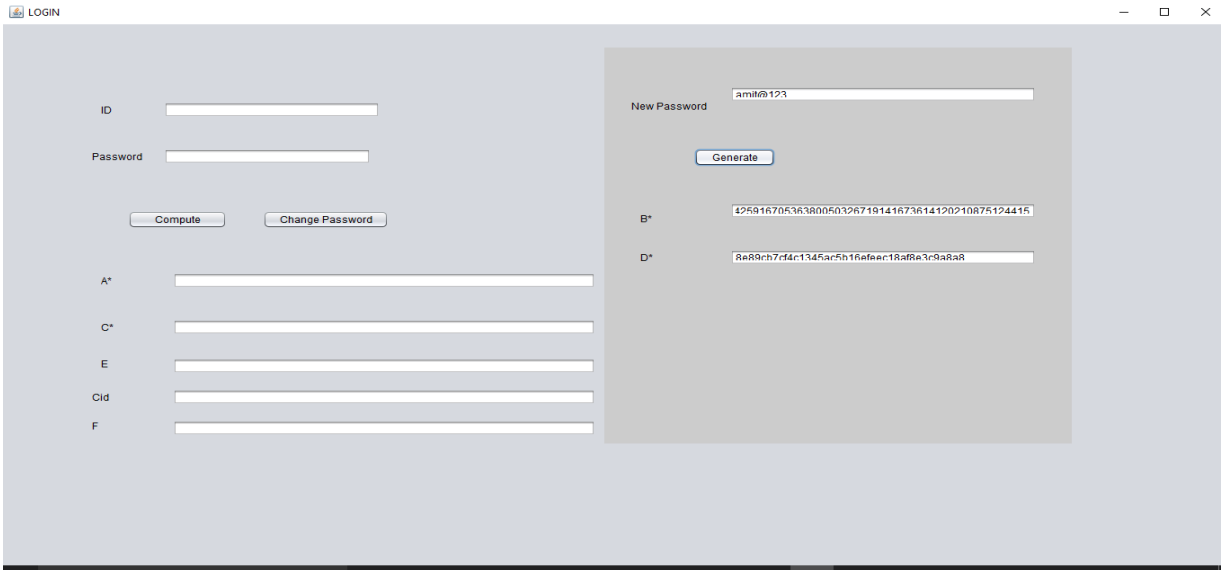

Figure 3. Shows that Generate New Computation key according new password

D. Session key Generation

In session key generation phase server verifies the user's unique id and password and relevant data which have entered by the user in the login phase.

If user id and password are correct and all the relevant data are valid or authenticate then server create a random key which is called a session key and server authorize(confirm) the user to do transaction**.**

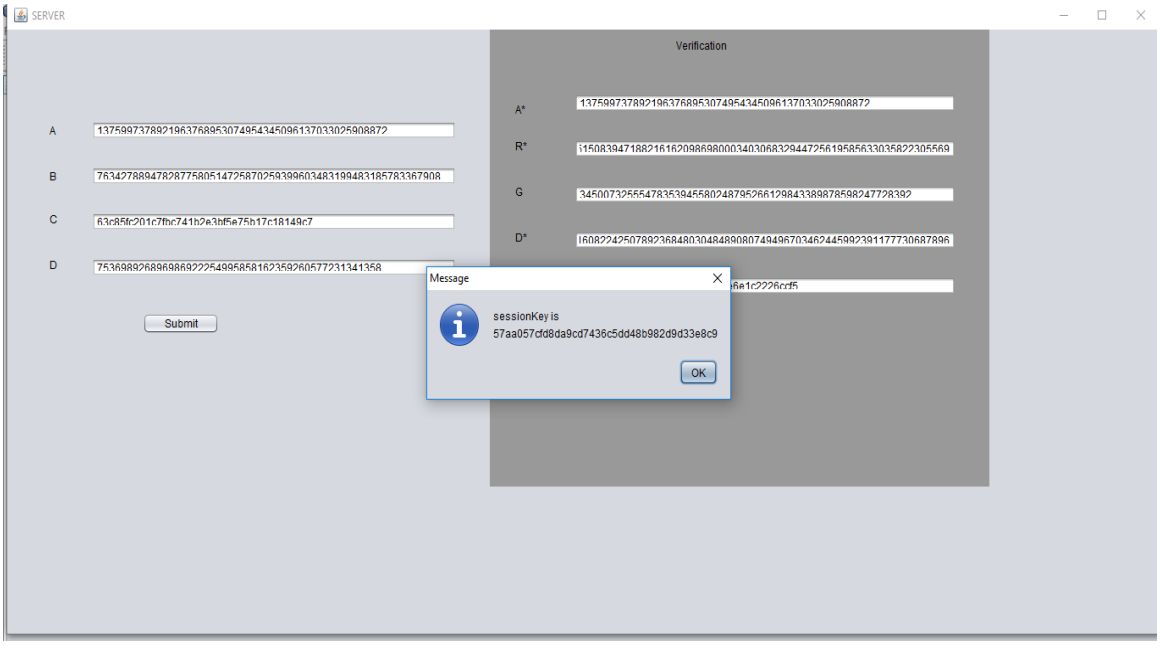

Figure 4. shows that Session key Generation process by server

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

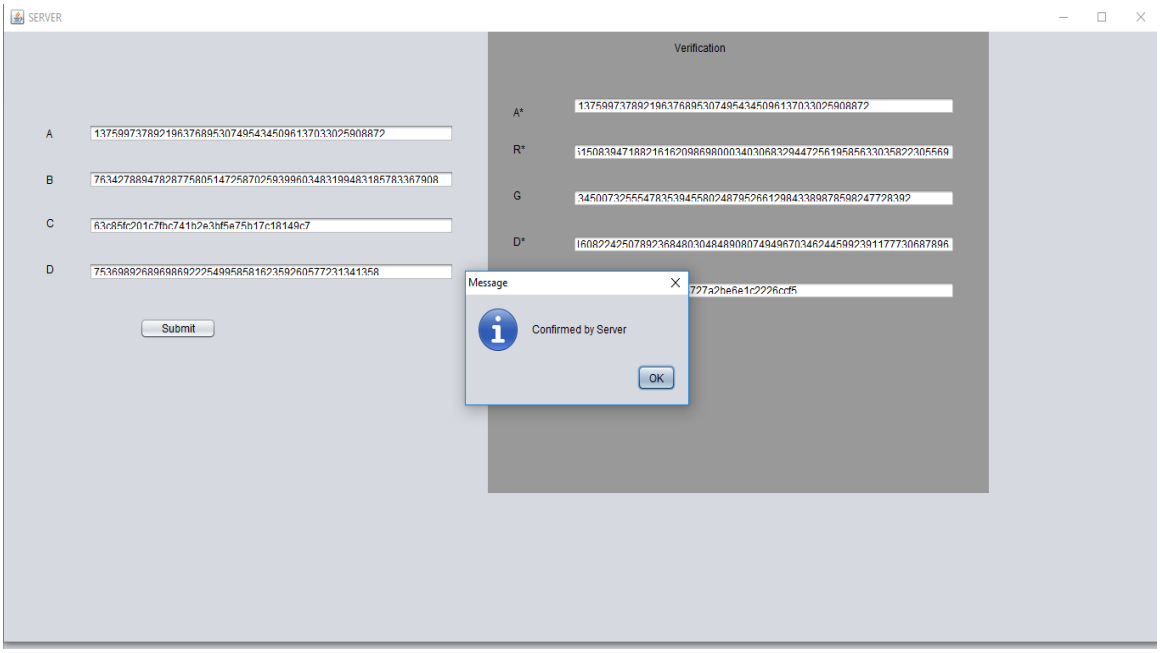

Figure 5. shows that Confirmation User process by server

V. Comparision With Existing Method

Table 1.
Prevention from Various Attacks

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

In above table shows the comparisons of different attack with existing scheme. Our proposed scheme prevents from different attack and secure all the phase like Registration, Login, Password change and Session key generation.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Table 2.
Time taken and No. of bit used

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

In above table shows our scheme take token of 32 bits, conceal value of 128 bit and time 12.540 which is better than existing scheme.

Table 3
Storage judgment of the planned scheme

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

In above table shows comparisons of storage judgment of planned scheme with existing work.

Table 4
Comparison of Computation with previous work

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	-	-

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.

In above table shows comparisons of Computation of planned scheme with existing work.it clearly shows that our scheme uses a less computation than existing work. Our scheme takes less time for computation and cost is cheaper than existing work.

VI. Conclusion

This dissertation revisited the privacy of 2-factor PAKA (Password Authenticate Key Agreement) protocols through sensible (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., challengers with pre-calculated data saved like (registration info, and other related information of account and user identification) in the sensible-card and challengers with different information (with respect to dynamic time slots) saved in the sensible (smart) card.

These challengers represent the potential threats (means of a determination to inflict harm on another) in distributed systems and are different which attention from both the academia and the industry. We also developed 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 verification has highlight the importance of elaborate or brief analysis the security models and general security analysis on the design of PAKA protocols using smart cards.

Simulation results points 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 PW) with fewer hash function and their combining. The main object of this dissertation is overcome the complexity and cost of the machine 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] R. Madhusudhan and Manjunath Hegde, "Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card", IEEE 2016.

[5] 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.

[6] 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.

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