International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

# An Efficient Trust Model for Online Application using 2-Factor Authentication and Token Based Authentication

**Varsha Jotwani[1], Dr. Amit Dutta[2]**

[1]Research Scholar, AISECT University, Department of Computer Science, Bhopal, India

[2]Deputy Director, AICTE, New Delhi, India

**Abstract:** ***Here in this paper security of E-commerce applications using an efficient Two Factor Authentication using Smart Card based Authentication and token based authentication is implemented which provides security from various attacks. Although various Trust Models are implemented for the security of E-commerce applications, but the techniques implemented takes more Storage Cost as well as suffers from User Revocation and Escrow Problem. Hence to overcome these limitations a new and efficient technique using Two Factor Authentications is implemented which not only minimizes the Storage Cost but also provides High User Revocation and Proxy Re- encryption.***

**Keywords:** Smart Card based Authentication; Token based Authentication; Encryption

## 1. Introduction

Security in computers is information protection from unauthorized or accidental disclosure while the information is in transmission and while information is in storage. Authentication protocols provide two entities to ensure that the counterparty is the intended one whom he attempts to communicate with over an insecure network. These protocols can be considered from three dimensions: type, efficiency, and security.

**Two Servers Password Authentication**

Two server authentication mechanisms are considered to be secure for authenticating a user in Internet based environment. As the number of services provided online is day by day increasing, users intending to use various online services are also increasing. With each service requiring the user to register separately, the overhead of remembering many user (Identity) ID /password pairs has lead to the problem of memorable. In this paper, proposed a two-server password authenticated key agreement mechanism using password where the user needs to recognize his secret key. The practical two-server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries.

**Two Server Systems**

The concept of a user id and password is a cost effective and efficient method. Identifying and allowing the authorized user to access the resources is one of the key aspects of authentication system. In today's computer era, there are so many vulnerabilities occurred based on internet. So, we have to design the application with high security. If there are any flaws, then it will be easily broken and an intruder can easily intrude.

A single server system is a system in which the password will be stored in a single server as shown in Figure 1. While considering the authentication system based on a single server, there are some drawbacks. The single server system is vulnerable to all sorts of attacks from intruders. The intruder can hack the system by trying all possible keys till the system gets compromised is the most successful in the single server system and exhaustive search also can be successful as shown in Figure 2.

## 2. Related work


**Figure 1:** Block Diagram of a Single Server System.

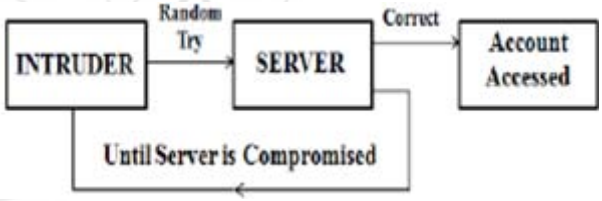


**Figure 2:** Example of single server system hacked by Intruder

Password authentication with smart card is one of the most convenient and effective two-factor authentication mechanisms for remote systems to assure one communicating party of the legitimacy of the corresponding party by acquisition of corroborative evidence. This technique has been widely deployed for various kinds of authentication applications, such as remote host login, online banking, e-commerce, and e-health [1]. In addition, it constitutes the basis of three-factor authentication [2]. However, there still exists challenges in both security and performance aspects due to the stringent security requirements and resource strained characteristics of the clients [3, 4].

Introduced the first remote user authentication scheme using smart cards there have been many of such schemes proposed

[5, 6, 7, 8 and 9]. One prominent issue in this type of schemes is security against offline guessing attack, which is the severest threat that a sound and practical scheme must be able to thwart. Traditionally, to prevent an adversary from launching offline guessing attack, one need to make sure that the scheme is not going to leak any information useful about the client's password to the adversary in the protocol run, even though the password is considered to be weak and low entropy. By observing this, many schemes employed some techniques similar to Bellovin and Merritt's Encrypted Key Exchange protocol.

A common feature of such schemes is that the smart card is assumed to be tamper-resistant, i.e., the secret parameters stored in the smart card cannot be revealed. However, recent research results have demonstrated that the secret data stored in the smart card could be extracted by some means, such as monitoring the power consumption or analyzing the leaked information [9]. Therefore, such schemes based on the tamper resistance assumption of the smart card are vulnerable to offline password guessing attacks, user impersonation attack, etc, once an adversary has obtained the secret data stored in a user's smart card and/or just some intermediate computational results in the smart card. Consequently, a stronger notion of security against offline guessing attack is developed to require that compromising a client's smart card should do not help the adversary launch offline guessing attack against the client's password.

In 2010, Pu [9] pointed out Yang et al.'s scheme is vulnerable to key compromise attack. Surprisingly, we found Yang et al.'s scheme still cannot achieve its claimed main security goal by demonstrating an offline password guessing attack in Appendix A, and through the security analysis of Yang et al.'s scheme, some subtleties and challenges in designing this type of schemes, different from the traditional password-based authentication, are uncovered.Despite of this, Yang et al.'s formal adversary model does capture the exact two-factor authentication of smart-card-based password authentication schemes: only with both the smart card and the correct password can a user carry out the smart-card-based password authentication scheme successfully with the remote authentication server.

Following Yang et al.'s seminal work, many enhanced schemes [10] have been proposed to address the smart card security breach problem, however, most of them were shortly found having various security weaknesses being overlooked [11, 12] Remarkably, even have been provided with a formal proof. The past thirty years of research in the area of password-authenticated key exchange (PAKE) has proved that it is incredibly difficult to get even a single factor based authentication scheme right, while the past decade of research in smart card based password authentication has proved that designing a secure and practical two-factor authentication protocol can only be harder

In SEC'12, Wang [11] observed that the previous papers in this area present attacks on protocols in previous papers and propose new protocols without proper security justification (or even a security model to fully identify the practical threats), which contributes to the main cause of the above failure. Accordingly, Wang presented three kinds of security models, namely Type I, II and III, and further proposed four concrete schemes, only two of which, i.e. PSCAb and PSCAV, are claimed to be secure under the harshest model, i.e. Type III security model.

Katz, Ostrovsky, and Yung (KOY) [13] demonstrated the first efficient PAKE protocol with a proof of security in the standard model. Their protocol was later abstracted by Gennaro and Lindell (GL), who gave a general framework that encompasses the original KOY protocol as a special case. These protocols are secure even under concurrent executions by the same party, but require a common reference string (CRS).

A different PAKE protocol in the CRS model is given by Jiang and Gong ,later abstracted and generalized by Groce and Katz [14]. Comparing to KOY/GL framework, the new JG/GK framework only requires a CCA-secure encryption scheme, and a CPA secure encryption scheme with an associated smooth projective hash function. It also achieves mutual authentication in three rounds. In their work Groce and Katz mentioned their framework will significantly improve efficiency when basing the protocol on lattice assumptions.Katz and Vaikuntanathan first instantiated the KOY/GL PAKE protocol under lattice assumptions.

In 2009 by S. Wanga, Z. Cao, K.-K. Choo, and L. Wang The first formal security model for authenticated key exchange protocols between two parties. The latter has been extended to the password-based setting with security analyses of the above 2-party password-based key exchange, under idealized assumptions, such as the random oracle and the ideal cipher models. Password-based schemes, provably secure in the standard model, have been recently proposed but only for two parties. papers considered password-based protocols in the 3-party setting, but none of their schemes enjoys provable security. In fact, our generic construction seems to be the first provably-secure 3-party password-based authenticated key exchange protocol [15] .

## 3. Proposed Methodology

We present a secure and an efficient ID-based remote user authentication protocol with smart card. We use one-way hash function and Bitwise XOR operation in this proposed scheme. Which execution time is extremely very low to compare to using Modular exponentiation. Our proposed scheme doesn't use any common key for encryption and decryption algorithm. Using one-way Hash function, it's computationally infeasible to invert operation. This scheme has four phases.

1) Registration phase
2) Login phase
3) Authentication/verification phase and
4) Password change phase.

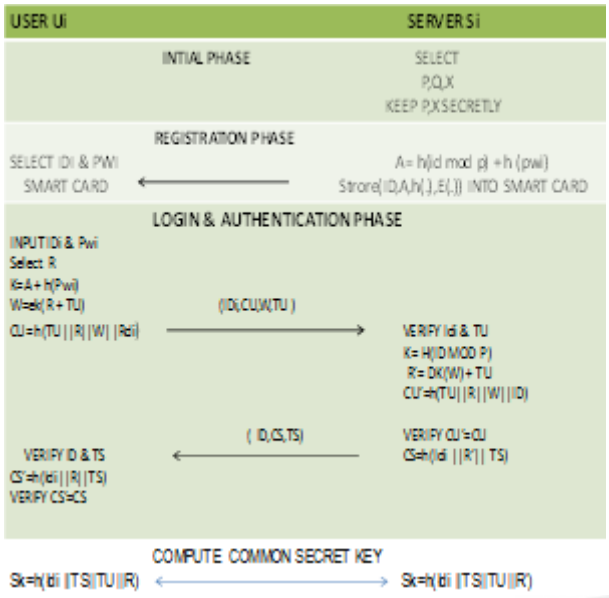


**Figure 3:** Cycle process of Smart Card Authentication

The notations use in proposed scheme and phases are describe below-
The Notations
U – Remote User
ID – Identity of User
PW– password chosen by User
S– Remote authentication Server
X– Permanent secret key of S
H (·) – One-way hash Function
xor – Bitwise XOR operation
|| – concatenation

**Registration Phase-**In the registration phase, User Ui wants to register himself/herself in remote server S. Firstly User chooses his/her ID and PW. Before register on Server, registration authority computes h (ID) and h (ID||PW) and sends to remote server S over a secure channel. Upon receiving the registration request from User Ui. Server S computes same parameters related to the User Ui. S computes
Ai= h (ID) xor h (X || h (ID))
Bi = Ai xor h (ID || PW)
Ci = h (Ai)
Di = h (ID || PW) xor h(X)

And stored some of them in the smart card memory and issues this smart card to User Ui. This smart card is delivered to User Ui through a secure channel.

**Login Phase-**This phase provides the facility of a secure login to the user .User wants to access same services on remote server S. first it gain the access right on the remote server S. User Ui inserts the smart card to card reader and keys in ID* and PW*. The card reader computes –

$$Ai^* = Bi \text{ xor } h (ID^* || PW^*)$$

And $Ci^* = h (Ai^*)$ and checks whether Ci (stored in the smart card memory) and $Ci^*$ are equal or not. If not, terminate to again login process. Otherwise yes, User Ui is legitimate bearer of the smart card. Then the card reader generates a random nonce Ri and computes –
Ei = Ai* xor Ri
Cid = h (ID || PW) xor Ri
Fi = h (Ai || Di || Ri || Tu)
Where Tu is current time when login request proceed. And send the login request massage {Fi, Ei, Cid, Tu, h (ID)} to remote server S.

**Verification Phase-** Upon receiving the login request massage {Fi, Ei, Cid, Tu, h (ID)}. Server verifies the validity of time delay between Tu‟ and Tu. Where Tu' is the travel time of the massage. Tu'-Tu ≤ ΔT where ΔT denotes expects valid time interval for transmission delay. Then server accepts the login request and go to next process, otherwise the server reject login request.
Server computes –
Ai* = h (ID) xor h (X || h (ID))
Ri* = Ai* xor Ci
G = h (ID || PW)* =Cid xor Ri
Di* = h (ID || PW)* xor h(X)
And computes F* = h (Ai* || Di* || Ri* || Tu)
And checks whether F and F* are equal or not. If they are not then reject the login request. If equal, then server S Computes–
Fs = h (h (ID) || Di || Ri || Ts) Where, Ts is remote server current time. And send acknowledge massage {Fs, G, Ts} to user Ui. Upon receiving acknowledge massage smart card compute

$$G^* = h (ID || PW)$$

Fs* = h (h (ID) || Di || Ri || Ts)
And checks where G =G*and Fs = Fs* are same or not. It is mutual authentication process. In which both Server and User verify to each other. If they are same then card reader makes session key (Sk) and both Server and User share it.
Sk = h (h (ID) || Ts || Tu || Ai)
Otherwise terminate to again login process.

**Password change Phase-**This phase is involved whenever User U want to change the password PW with a new Password PWnew .User U inserts the smart card to the card reader/client machine and keys in ID* and PW* and request to change password. The card reader checks whether C = C* are equal or not. If it is satisfy User U is a legitimate bearer of the smart card. Then the card reader asks the User Ui to input new password PWnew. After entering the new password the card reader calculate-
Bnew = Ai xor h (ID || PWnew) and
Dnew = h (ID || PWnew) xor h (ID || PW) xor Di
And change B with Bnew and D with Dnew in smart card memory.

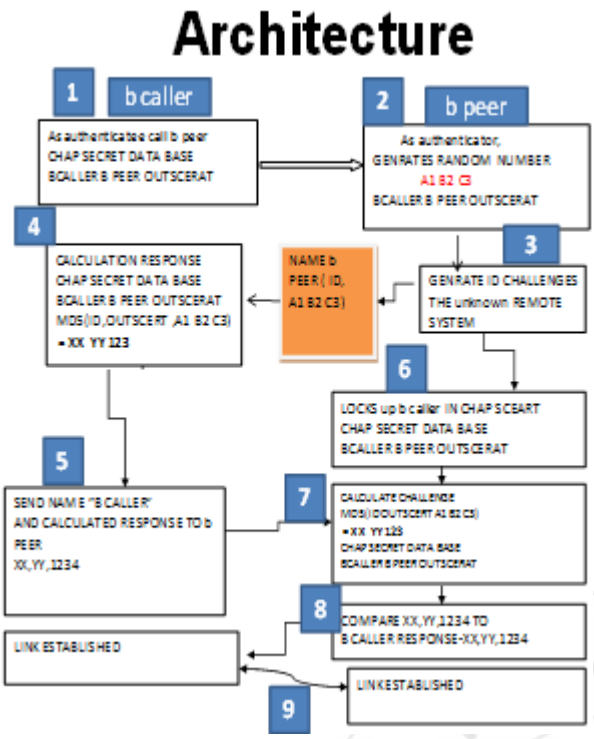


**Figure 4: Token Based Authentication**

## 4. Result Analysis

As shown in the table 1 is the prevention of our proposed work from various attacks in the attack.

**Table 1:** Prevention of various attacks

| Replay attack | Identity disclosure attack | Insider attack | Outsider attack | Eaves dropping | Identity Spoofing | Password based attack | Man-in the middle |
|---|---|---|---|---|---|---|---|
| YES | YES | YES | YES | YES | YES | YES | YES |

As shown in the table 2 is the analysis of first factor authentication. Here the number of bits generated in secrete value depends on the number of bits taken in token.

**Table 2:** First factor authentication

| *Number of bits in token* | *Number of bits in secrete value* | *Time taken* |
|---|---|---|
| 32 | 128 | 10.437 sec |

Table 3 shows, the storage comparison of the proposed scheme with the relevant user authentication based on smart card, Which shows our proposed scheme is reduced burden on the server, because the Server has store only server secret key (X).

**Table 3:** Storage comparison of proposed Scheme

| Storage/ scheme | Our scheme | R. song al et. |
|---|---|---|
| Smart card | 480 bits | 320 bits |
| Server | 160 bits | 480 bits |

The Table 4 shown below is the analysis and comparison of prevention from various attacks during the authentication between user and server. The existing methodology implemented here for the authentication between user and server using Elliptic Curves provides security from various attacks while the mutual authentication technique implemented is still vulnerable to certain attacks. The proposed methodology implemented on Data Sharing on Public Clouds using Signcryption prevents from various attacks just because of the Hardness of the Algorithm since the algorithm is based on Hard Logarithmic Problem hence it is secure against various security attacks in Cloud Computing.

**Table 4:** Analysis of Prevention from Various Attacks

| *S. No.* | *Security Attacks* | *Existing Work* | *Proposed Work* |
|---|---|---|---|
| 1 | Password Impersonation | No | Yes |
| 2 | Password Guessing Attack | Yes | Yes |
| 3 | Confidentiability | No | Yes |
| 4 | Public Verifiability | Yes | Yes |
| 5 | DoS Attack | Yes | Yes |
| 6 | Insider Attack | No | Yes |
| 7 | Denning Sacco Attack | Yes | Yes |
| 8 | DDoS Attack | No | Yes |
| 9 | Outsider Attack | Yes | Yes |
| 10 | Online Dictionary Attack | Yes | Yes |
| 11 | Offline Dictionary Attack | Yes | Yes |
| 12 | Server Masquerade Attack | Yes | Yes |
| 13 | Integrity | Yes | Yes |
| 14 | Unforgeability | Yes | Yes |
| 15 | Non-Repudiation | Yes | Yes |
| 16 | Forward Secrecy | Yes | Yes |
| 17 | Additional Authentication | No | Yes |

## 5. Conclusion

The Proposed methodology implemented here for the Security of E-commerce applications using 2 Factor Authentication such as Smart Card based Authentication and Token based Authentication. The Methodology implemented provides security from various attacks and also provides less Storage Cost and Storage Space. The Methodology implemented is then compared with some of the existing methodologies that are implemented for the security of E-commerce applications. Experimental results on the basis of Various Parameters such as Storage Cost and Security Attacks proves the efficiency of the proposed methodology.

## References

[1] Chen, C.L., Lu, M.S., Guo, Z.M.: A non-repudiated and traceable authorization system based on electronic health insurance cards. Journal of Medical Systems pp. 1–12, doi: 10.1007/s10916-011-9703-4, 2011.
[2] Huang, X., Xiang, Y., Chonka, A., Zhou, J., Deng, R.: "A generic framework for three-factor authentication: preserving security and privacy in distributed systems. Parallel and Distributed Systems", IEEE Transactions on 22(8), 1390–1397, 2011.
[3] Chen, T., Hsiang, H., Shih, W.: "Security enhancement on an improvement on two remote user authentication schemes using smart cards", Future Generation Computer Systems 27(4), 377–380, 2011.
[4] Chen, Y.L., Chou, J.S., Huang, C.H.: "Improvements on two password-based authentication protocols".

Cryptology ePrint Archive, Report 2009/561, http://eprint.iacr.org/2009/561.pdf, 2009.
[5] Khan, M., Kim, S., Alghathbar, K.: Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme'. Computer Communications 34(3), 305–309, 2011.
[6] Li, C.T., Lee, C.C.: "A robust remote user authentication scheme using smart card" Information Technology And Control 40(3), 236–245, 2011.
[7] Ma, C.G., Wang, D., Zhang, Q.M.: "Cryptanalysis and improvement of sood et al.s dynamic id-based authentication scheme",In: Ramanujam, R., Ramaswamy, S. (eds.) ICDCIT'12, LNCS, vol. 7154, pp. 141–152. Springer-Verlag, 2012.
[8] Kasper, T., Oswald, D., Paar, C."Side-channel analysis of cryptographic rfids with analog demodulation". In: Juels, A., Paar, C. (eds.) RFIDSec'12, LNCS, vol. 7055, pp. 61–77. Springer Berlin / Heidelberg, 2012.
[9] Pu, Q.,"An improved two-factor authentication protocol". In: 2010 International Conference on Multimedia and Information Technology (MMIT). vol. 2, pp. 223– 226. Ieee, 2010.
[10] Shim, K.:" Security flaws in three password-based remote user authentication schemes with smart cards". Cryptologia 36(1), 62–69, 2012.
[11] Wang, Y.G.: "Password protected smart card and memory stick authentication against off-line dictionary attacks". In: Gritzalis, D., Furnell, S., M., T. (eds.) SEC 2012, IFIP AICT, vol. 376, pp. 489–500. Springer Boston availe at http://coitweb.uncc.edu/ yonwang/papers/smartcard.pdf, 2012.
[12] Xie, Q.: Dynamic id-based password authentication protocol with strong security against smart card lost attacks. In: Snac, P., Ott, M., Seneviratne, A., Akan, O. (eds.) Wireless Communications and Applications, LNICST, vol. 72, pp. 412–418. Springer Berlin / Heidelberg, 2012.