Elliptic Curve Cryptography based Secure and Efficient Authentication Protocol for Smart Card Users

Javed R. Shaikh, P. Vijayakumar, R.Yuvaraj,Sarang Patil

***Abstract**: Communication scheme which is used to have communication between authorized remote users over an insecure network is generally the authentication scheme which uses the password for the authentication. Remote user authentication techniques using the smart card have been proposed by many researchers. The main benefit of using the smart card is the storage availability and the computation speed. Huang et al. proposed a scheme for user authentication with smart cards which uses the concept of the timestamp. In Huang et al.'s protocol authors argued that their protocol is secure and efficient against any type of attack. Unfortunately Jung et al. show that Huang et al.'s model fails against the offline password guessing attack and with this scheme wrong password detection is not easy. In Huang et al.'s scheme, RSA cryptosystem is used to offer the authentication. In this article, advanced and secure smart card based authentication protocol using elliptic curve cryptography (ECC) is proposed. This proposed scheme thus overcomes all the possible drawbacks of Huang et al.'s scheme, and it has faster computation as compared to the available schemes*

***Keywords**: ECC; E-commerce; Smart Cards; Security Protocols; User authentication.*

I. INTRODUCTION

With the increased use of the internet for everyday activities like Electronic Commerce (E-commerce) services and remote host login user want to access the services from remote locations. Many available remote authentication schemes focus on preservation of user anonymity from the eavesdropper. The authentication schemes used in E-commerce requires anonymity not only to the authentication server but also to the eavesdropper [1]. While accessing the network services from the remote location user authentication is an essential part of the security requirement for protecting the systems and the network.

Till date, many research scholars have proposed different authentication schemes for the remote user to validate legitimate user and servers. First novel password-based authentication scheme used for the remote access control has been proposed by the Lamport et al. in the year 1981. After this scheme, many authors proposed various user authentication schemes. Yang and Sheih [2] proposed a new authentication scheme for the users using the timestamp in 1999, where authors claimed that using this scheme, users can very easily select and alter their password according to their liking. Later in the year, 2003 modified Yang and Sheih scheme was proposed by Shen et al. [3] which is not affected by the forge login attack, and it offers a secure and safe authentication. But according to Liu et al. [4] and Awasthi et al. [5] Shen et al.'s scheme is not secure against forged login attack. To overcome above said problems Liu et al. [4] suggested nonce based user authentication scheme. Then in the year 2011 Awasthi et al. [5] presented an improved scheme for authentication where non-storage of data on the server side is taken care. In recent times, Huang et al.'s [6] indicate that the scheme of Awasthi et al. is not secure if impersonation attack is there and so Huang et al. projected a scheme using the timestamp to have secure user authentication with a smart card. In this proposed model no verification information for the users is required by the remote server. However, Jung et al. [7] has performed the cryptanalysis for Huang et al.'s authentication model and found that this scheme is susceptible to the off-line password guessing attack and during login phase detection of the wrong password is not that easy task. Jung et al. also pointed that in Huang et al.'s scheme during the password change phase it is insecure to change the password of the user.

Here with this paper an advanced and enhanced timestamp based authentication protocol for the remote user is proposed which overcomes all the limitations of Huang et al.'s design highlighted by the Jung et al. The proposed scheme utilizes the elliptic curve cryptography which is suitable for smart cards applications as it needs small key size and computation speed is also high as compared to RSA which is used by the Huang et al.'s scheme. The remaining paper is structured as follows: Section II, highlights overview of the Huang et al.'s authentication design [6]. The security analysis performed by Jung et al. is given in section III. The proposed authentication schemes using ECC is presented in section IV, and at last in section V the analysis of proposed protocol is presented by considering its security parameters. In last part, some conclusions will be made.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Javed R.Shaikh*, Assistant Professor, Department of Electonics and Telecommunication, SKN Sinhgad Institute of Technology and Science, Lonavala, India.

P.Vijayakumar, Associate Professor, School of Electronics Engineering, VIT University, Chennai, Tamilnadu, India..

R.Yuvaraj,Assistant Professor (SG) Saveetha school of Engineering ,Chennai, India.

Sarang Patil, Assistant Professor, ,Department of Electonics and Telecommunication, SKN Sinhgad Institute of Technology and Science, Lonavala, India.

Retrieval Number: A7115119119/2019©BEIESP
DOI: 10.35940/ijitee.A7115.129219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. OVERVIEW OF HUANG ET AL.'S PROTOCOL

In this section general review of Huang et al.'s authentication protocol with smart-card is given, which is proposed in 2013. Huang et al.'s scheme uses the timestamp based authentication for the user. This scheme has four different phases. The details of various phases are explained below.

A. Initialization Phase

During this phase of Huang et al.'s scheme, the trusted authority which is responsible to generates universal parameters is the Key Information Centre (KIC). KIC is also used to compute user's undisclosed information and distributes smart cards to the new users.

During this phase following steps are performed by the Key Information Center:

1) Generates two random large prime numbers p, q and calculates $n = p*q$.
2) Selects two integers e and d such that $e \cdot d$ mod $(p - 1)$ $(q - 1) = 1$, where e *is* public key and d is private key of the system.

B. User Registration Phase

Fig.1 shows the diagrammatic representation of registration phase.

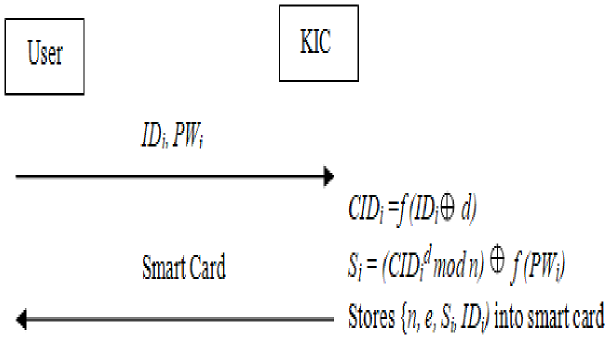
User
KIC
ID_i, PW_i
$CID_i = f(ID_i \oplus d)$
Smart Card
$S_i = (CID_i^d \bmod n) \oplus f(PW_i)$
Stores $\{n, e, S_i, ID_i\}$ into smart card

Fig. 1.User Registration Phase.

First time Registration of user Ui to the server S is performed as explained below:

1) U_i provides identifier which is ID_i and password PW_i to KIC using a secure communication medium.
2) After getting the ID_i and PW_i from the user, *KIC* calculates identifier of the smart card $CID_i = f(ID_i \oplus d)$, and hidden information $S_i = (CID_i^d \bmod n) \oplus f(PW_i)$.
3) Details *of* $\{n, e, S_i, ID_i\}$ are stored into a smart card by KIC, and then the card is given to the user U_i using a protected communication medium.

C. Authentication and Login Phase

The diagrammatic representation of this phase is depicted in Fig. 2. The following steps will carry out when user Ui tries to login and authenticate to the server S.

1) User U_i inputs password PW_i and finds X_i and Y_i as shown below: $X_i = S_i \oplus f(PW_i)$ and $Y_i = X_i^{f(IDi,\, Tc)} \bmod n$, where T_c denotes user sides present timestamp.
2) Then U_i conveys its login request to the server S by providing a messages $M = \{ID_i, n, e, T_c, Y_i\}$.

On the server side once the message M is available at time T_s, the smart card executes the following operations:

1) Server S checks the ID_i to find out the genuine user and verifies the condition $|T_s - T_c| < \Delta T$ using the timestamp T_s in the received message, where ΔT denotes expected the amount of delay during the transmission. If this condition is true, then the login request of the user is processed, and if the condition fails, then server rejects this request.
2) Server S calculates $CID_i = f(ID_i \oplus d)$ and finds $Y_i^e = f(ID_i \oplus d)^{f(IDi,\, Tc)} \bmod n$. If the condition is true, then the server S completes the request from a user to login, and if the condition fails then server rejects this request.
3) Then server S compute $R = (f(ID_i, T_s'))^d \bmod n$, and convey $M' = \{R, T_s'\}$ to U_i, where T_s' is a server sides present timestamp on the.
4) When at the user side reply message M' is received at time T_c', the U_i verifies the timestamp T_s' in the message using condition $|T_s' - T_c'| < \Delta T$, where ΔT is delay expected during transmission. With the validation of condition, the user U_i agrees to the login respond of S. If the condition fails, it ends the whole process.
5) User U_i computes $R' = R^e \bmod n$ and verifies the condition for $R' = f(ID_i, Ts')$. If the equation is satisfied, then the user U_i accepts the server S. Otherwise, rejects it.

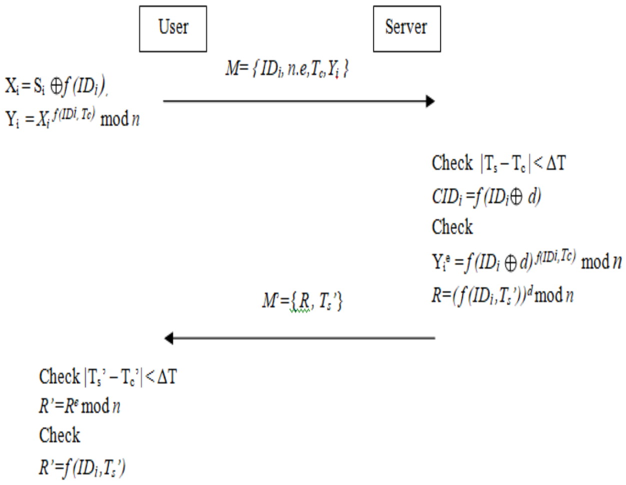
User
Server
$X_i = S_i \oplus f(ID_i)$
$Y_i = X_i^{f(IDi,Tc)} \bmod n$
$M = \{ID_i, n.e, T_c, Y_i\}$
Check $|T_s - T_c| < \Delta T$
$CID_i = f(ID_i \oplus d)$
Check
$Y_i^e = f(ID_i \oplus d)^{f(IDi,Tc)} \bmod n$
$R = (f(ID_i, T_s'))^d \bmod n$
$M' = \{R, T_s'\}$
Check $|T_s' - T_c'| < \Delta T$
$R' = R^e \bmod n$
Check
$R' = f(ID_i, T_s')$

Fig. 2.Authentication and Login Phase.

D. Authentication and Login Phase

Fig.3 describes the process of changing the password. The user can alter the required password easily without the concern of remote server S.

During this phase, the user Ui needs to alter old password PWi with as new password PWi' by executing the following steps:

1)= The user U_i needs to choose a new password PW_i'.

2) U_i Calculate $S_i' = S_i \oplus f(PW_i) \oplus f(PW_i')$.
3) Smart card replaces S_i with S_i', which means that the password change is completed successfully.

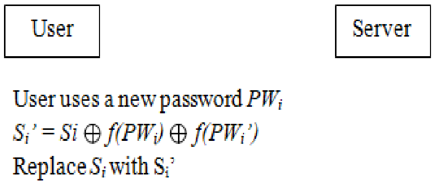
User
Server
User uses a new password PW_i
$S_i' = Si \oplus f(PW_i) \oplus f(PW_i')$
Replace S_i with S_i'

Fig. 3. Password changing phase

III. SECURITY ANALYSIS OF HUANG ET AL.'S PROTOCOL

This section highlights the drawbacks of Huang et al.'s user authentication model which are pointed out by the Jung et al. According to Jung et al. the authentication model presented by Huang et al.is not safe against off-line password guessing attack. During login phase, if the user Ui submits an incorrect password PWi, the login and authentication phases are still carried out until server S checks it. The details of these flaws highlighted by Jung et al. are described as follows.

A. Off-Line Password Guessing Attack

In Huang et al.'s scheme, an attacker can get the secrets {n, e, Si, IDi} in the smart card if an attacker got the smart card. With this card, an attacker can easily find the request message {IDi, n, e, Tc, Yi} for the login between a user and the server. And then, attacker imparts the off-line password guessing attack easily. So Huang et al.'s design is defenseless if offline password guessing attack is imparted.

B. Slow In Detecting The Wrong Password

During login phase of Huang et al.'s design, when user Ui inputs IDi and PWi, the smart card will not validate the user's password by itself. As a result, when user Ui inputs invalid password by mistake, the authentication and login phases are still carried out until server S does the validation of password. This drawback results in the needless wastage of computation and communication costs during login phase.

C. Weakness in Password Change Phase

If any unauthorized user gets the access to the smart card, then that user can easily set the desired password by replacing old password in password changing phase as there is no communication required with the server while changing the password. To change the password, an unauthorized user inserts Ui's smart card into its reader and then submits the details of IDi and PW*, where PW* is unauthorized user's random new password, and finally, it requests to alter the password.During the process of altering the password, the unauthorized user gives random password PW*. The smart card then computes $Si^* = Si \oplus f(PWi) \oplus f(PW^*)$, which results in CIDid $\oplus$ f (PW*). After this calculations, smart card replaces Si with Si* without any verifying it. Therefore, changing the password is insecure in Huang et al.'s scheme.

IV. PROPOSED AUTHENTICATION PROTOCOL

As Huang et al.'s scheme has drawbacks, a more competent and more secure protocol for the user authentication using ECC is proposed here. The proposed authentication protocol employs one-way hash function instead of a costly cryptosystem. Also, the RSA cryptosystem is replaced by the ECC. Table I shows the various notations used in the protocol. This protocol has the same phases: as explained for the Huang et al. scheme in section II.

Table- I: Different Notations used in Proposed Protocol

Notations	Meaning
U_A	User
S	Server
k	The security parameter
q	A big prime number
F_q	A field having prime order of q
E_q (a,b)	A set of elliptic curve points of order n, where a; b ϵ Fq
Q	A base point of order n over E_q (a,b)
$d_i : U_i$	The private/public key pair of the entity i, where i = A,S where d_i ϵ Z_q and $U_i = d_i$ *Q
H ( )	One-way cryptographic hash function
‖	The message concatenation operator
E (·)	The scalar point multiplication on the elliptic curve
A	The Adversary

A. System Initialization Phase

In the system initialization phase, server S initializes system by selecting following parameters.

1) Select a finite field F_q over q > 2160.
2) Select an elliptic curve such as E_q (a,b) : y^2 mod q = x3+ax+b mod q having order n over F_q,
3) Select a point q having order n over elliptic curve Eq (a,b)
4) Publish E_q (a,b) and value of Q
5) User A and server S select their private and public keys as (d_A:U_A) and (d_S :U_S) where U_A= d_A*Q and U_S =d_S*.Q

B. Registration phase

In this phase following procedure is adopted

1) User U_A sends ID_A and PW_A to the server S.
2) Then Server S calculates H_A = H (PW_A‖d_S) and R_A= H_A* Q.
3) Server Stores { ID_A,R_A,H(.),E_q,Q} on smart card .

C. Login phase

In this phase following procedure is followed by the card user to login to the server.

1) User U_A selects the current timestamp as T_A and inputs identity ID_A and Password PW_A.
2) User U_A Calculates K_A=d_A*U_S.
3) Then user U_A computes C_A = H (T_A‖ID_A‖ K_A‖ R_A).
4) User conveys login request with the message M to the server as M={ ID_A, C_A, T_A, R_A}.

D. Authentication phase

Once the message having login request is received from the user, the server S performs the following procedure to authenticate the user.

1) Server S selects current timestamp as T_S and checks for the condition that (T_S - T_A) ≤ ΔT, where ΔT is the expected time delay.
2) Server S computes the value of $K_A = d_S * U_A$.
3) Then Server S computes $\overline{C_A}$ = H ($T_A \| ID_A \| K_A \| R_A$) and checks $C_A=?\ \overline{C_A}$, If condition satisfies then the server sends authentication pass message to the user otherwise it rejects the login request.
4) Then Server S computes C_S = H ($ID_A \| K_A \| T_S$) and sends message M ={ ID_A, C_S, T_S }to the U_A.

After getting authentication pass message from server user checks for the authenticity of the server.

5) User U_A computes $\overline{C_S}$ = H ($ID_A \| K_A \| T_S$) and checks $C_S=?\overline{C_S}$, If condition satisfies then the server is authenticated, and the session key is established.Session key K = H ($T_S \| ID_A \| K_A \| R_A$)

As explained above the login and authentication procedure is adopted among the remote server and the smart card while establishing the secure communication.

To define the efficiency and communication of the proposed scheme we have used notations to analyze the computational complexity of proposed protocol compared to other protocols. The notation T_E refers to the time taken for one modular exponentiation, T_M denotes the time required for the computation of one modular multiplication, T_H means the time for executing the hash function, and TPM denotes the time complexity for executing the elliptic curve point multiplication. Table II shows the comparison of computation times taken by various schemes.

As shown in table II the Huang et al.'s protocol is efficient than the Awasthi et al.'s protocol where each user needs to perform two modular exponentiation (T_E), and two hash function computation (T_H) for the authentication purpose and for the server authentication Huang et al.'s protocol needs three modular exponentiation (T_E) and two hash function computation (T_H).

TABLE- II: Comparison of Computational Cost for Various Schemes

Schemes	Computations for user to complete authentication	Computations for server to complete authentication
Awasthi et al.'s	$3T_E + 3T_M + 2T_H$	$3T_E + 1T_M + 3T_H$
Huang et al.'s	$2T_E + 2T_H$	$3T_E + 2T_H$
Proposed Scheme	$2T_{PM} + 3T_H$	$3T_{PM} + 4T_H$

In the proposed protocol, the user requires Two point multiplication (T_{PM}) and three hash function computations (T_H) to achieve its authentication, and on the other side, the server needs three point multiplication (T_{PM}) and four hash function computations (T_H) for its authentication. In the proposed scheme instead of RSA cryptosystem ECC is used so this scheme does not require the modular multiplication and modular exponentiation. The time needed for modular multiplication and modular exponentiation is higher than the time needed for point multiplication on an elliptic curve. Therefore, the proposed authentication method is more efficient than the Huang et al.'s protocol.

V. SECURITY ANALYSIS OF PROPOSED PROTOCOL

The security analysis of new protocol is demonstrated to highlight its security strength concerning various types of security attacks.

A. Security of the system secrets

As the ECC is used in this proposed protocol, it is difficult for the attacker to find the secret stored at the server side as well as the user side. For an attacker to have access to stored secret, it is necessary to solve the elliptic curve discrete logarithm problem (ECDLP) [8]. The difficulty in solving ECDLP makes it harder to break the system secret.

B. Security of the stored data

In this authentication scheme, the secret stored on the smart card is RA. Which is RA= HA*Q. Along with RA card has the details of ID. If attacker extracts RA from the smart card, then attacker needs to find HA otherwise it is difficult to find any information about the password. So due to use of elliptic curve point multiplication the user can easily achieve the security of stored data on the card.

C. Security of the Password

As in the authentication protocol only available information for the intruder is {IDA, RA, TA, CA} and {IDA, CS, TS}. It is very difficult to solve the value of password from this available information. To extract the password intruder needs to calculate the ECDLP. As ECDLP is hard to break so, the user can secure his/her password with this scheme. Along with ECDLP one way hash functions are also used to secure the user password.

The analysis of proposed protocol considering its security against various online attacks is given below.

A. Impersonation attack

According to the definition, the impersonation attack is a type of attack where a third party assumes the uniqueness of one of the genuine entities in a system or a communication protocol. The designed protocol is capable of handling impersonation attack on both the user and server side.

On the user side as only IDA and RA is available to the attacker it makes attacker difficult to recover the card password as the attacker needs to solve the ECDLP problem. On the server side also attacker cannot get the access to the private key of the server, so there is no effect of impersonation attack.

B. Replay attack

In this kind of attack, adversary repeats the valid data transmission by continuous retransmitting it. As in the proposed scheme timestamp method is used, if the adversary repeats the data transmission, then server checks the received timestamp. By verifying the timestamp, the server can simply detects the replay attack.

C. Modification attack

In proposed protocol, each authentication message from the user to the server and vice versa is protected with the one way hash function along with the timestamp. After the hashing, the hash value is encrypted using the ECC. If an unauthorized person desires to modify the data, then that person needs to solve the ECDLP problem. So with a proposed design for authentication intruder cannot easily modify the data.

D. Man-in-the-middle attack

It is the active type of attack where the attacker secretly relays and attacks the communication system between two entities who believe they are directly communicating with each other. In this proposed protocol if the attacker knows the value of RA still he cannot find the password as it is first hashed with the secret key of the server.

VI. CONCLUSION

To provide the user authentication using smart card Huang et al. has proposed their protocol. However, the protocol proposed by Huang et al. has some vulnerability such as their scheme cannot sustain against the offline password guessing attack. Also with their scheme wrong password detection during the login phase is not possible. In Huang et al.'s scheme, the computation time required is more as it uses the RSA cryptosystem.

In this paper secure and efficient user authentication protocol is proposed which uses the smart card based user authentication using elliptic curve cryptography. In the proposed scheme instead of RSA cryptosystem ECC is used so this scheme does not require the modular multiplication and modular exponentiation. Therefore, the proposed authentication method is more efficient than the Huang et al.'s protocol. The proposed user authentication design is secure against the various online attacks such as impersonation attack, replay attack, modification attack and man in middle attack. Using the proposed protocol we can easily identify the wrong password entered during login phase.

REFERENCES

1. Y. Liu, Z. Zhao, H. Li, Qun Luo and Y. Yang, "An Efficient Remote User Authentication Scheme with Strong Anonymity" International Conference on Cyberworlds, 2008.
2. W. W. Yang and S. P. Shieh, "Password authentication scheme with smart cards," Computers and Security, Vol. 18, No. 8, pp. 727-733, 1999.
3. J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication," Computers and Security, Vol. 22, No. 7, pp. 591-595, 2003.
4. J. Y. Liu, A. M. Zhou, and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," Computer Communications, Vol. 31, pp. 2205-2209, 2008.
5. K. Awasthi, K. S. Srivastava, and R. C. Mittal, "An improved timestamp-based remote user authentication scheme," Computers and Electrical Engineering, Vol. 37, pp. 869-874, 2011.
6. H. F. Huang, H. W. Chang, and P. K. Yu, "Enhancement of timestamp-based user authentication scheme with smart card," International Journal of Network Security, Vol. 16, No. 6, pp. 463-467, 2013.
7. J. Jung, Y. Choi, Donghoon Lee, J. Kim, and D. Won, "Security Weaknesses of a Timestamp-Based User Authentication Scheme with Smart Card", International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015.
8. R. Song, "Advanced smart card based password authentication protocol", Computer Standards & Interfaces, 321–325,2010.

AUTHORS PROFILE

Dr. Javed Shaikh received the Bachelor of Engineering degree in Electronics and Telecommunications from Dr. BAMU University, India in 2009 and Master of Engineering in VLSI and Embedded System from Pune University in 2012. He has received his PhD degree in communication networks from Technical University of Sofia (TUS), Bulgaria. He is with the Department of Electronics and Telecommunication, SKN Sinhgad Institute of Technology and Science, Lonavala, Pune from 2013 as an Assistant Professor. His interests are in communication networks, cryptography and its real time applications, cyber security and E-commerce systems. He has been working on systems for elliptic curve cryptography applications in E-commerce and IOT.

Dr. P. Vijayakumar is currently working as Associate Professor in School of Electronics Engineering at VIT university Chennai campus, India and completed his Ph.D in Wireless Security at Pondicherry University during 2015. He has totally 12 years of teaching and research experience and published more than 40 research papers in SCOPUS /SCI Indexed National / International Journals and Conferences. His area of specialization is Elliptic and Hyperelliptic Curve Cryptography, Blockchain technology, Cryptography and Network Security, Cryptographic Algorithms, DNA Steganography, Embedded System and IoT.

Mr.R.Yuvaraj is currently working as Assistant Professor in School of Electronics Engineering at Saveetha School Engineering , Chennai, India and completed his M.E in Computer and communication Engineering at Dr Paul's College of engineering, Anna University during 2009. He has totally 15 years of teaching and research experience and published more than 20 research papers in SCOPUS /SCI Indexed National / International Journals and Conferences. His area of specialization is wireless Communication, IOT, Machine learning and Cryptography and Network Security.

Dr.Sarang Patil is currently working as Assistant Professor in Department of Electronics and Telecommunication, SKN Sinhgad Institute of Technology and Science, Lonavala, Pune from 2014. He has totally 10 years of teaching and research experience and published more than 15 research papers in National / International Journals and Conferences. His interests are in communication networks, Antenna Design, Microwave Engineering.