PROVABLY SECURE TWO-FACTOR AUTHENTICATION SCHEME FOR E-HEALTH USING SMART CARD

Dr. B. INDRANI,
Assistant Professor,
Department of Computer Science,
Directorate of Distance Education
Madurai Kamaraj University
Madurai-21

M. KARTHIGAI VENI,
Assistant Professor,
Department of Computer Applications,
Yadava College, Govindarajan Campus,
Tiruppalai
Madurai-14

Dr. M. AMUTHA PRABAKAR,
Associate Professor and Head,
Department of CSE,
R. V. S. College of Engineering,
Dindigul, Tamil Nadu, INDIA

Abstract

Nowadays, IT enabled service gain more attention due to easy to access resources from remote place. IT enabled services are extend their service to all kind of business and personal related applications like, e-commerce, e-business, e-transactions and e-healthcare etc.,. In India, e-healthcare system gains more attention in recent years due to its effectiveness. We have to consider information assurance is an important part of e-healthcare system, because maintaining of sensitive health records of individuals. Any information system is subject to two different issues, 1) information handling and 2) information assurance. An e-healthcare system has to provide necessary security factors without compromising information loss. Information access is one of the foremost issue for providing access rights to the legal users. In this paper, we have proposed a two factor authentication scheme using Elliptic Curve Cryptography with smart card. The proposed authentication is based on two-factor authentication with smart card and password, which provides high security with minimum computational cost. The proposed scheme generates new session key for every new session with fresh time stamp and nonce value. The proposed scheme needs minimum computation cost compared with the related authentication schemes using smart card.

Key words: smart card, authentication, password, e-healthcare, public-key cryptosystem, ECC, Session Key

I. INTRODUCTION

E-healthcare system gains more attention in recent years due to increasing number of patient day by day. In E-healthcare system needs multi-dimensional view for implementing as a real time application. We have to answer the following questions in front of us, how to store, what are the computational facility we need to develop the system and what are the security measures we have taken. In any kind of information system development, we need to clear two points information storage and information assurance. The information assurance is one of the key research areas in most of the information system. E-healthcare system is one best example of information system. In recent years, lot of research activities and articles has been published by the research peoples. Information Assurance is assuring information availability and managing the risk related to information processing, storage, access, etc., Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. Information Assurance (IA) is the process of getting the right information to the right people at the right time. The information assurance process typically begins with the enumeration and classification of the information assets to be protected. Next, the IA practitioner will perform a risk assessment for those assets. Vulnerabilities in the information assets are determined in order to enumerate the threats capable of exploiting the assets. The assessment then considers both the probability and impact of a threat exploiting a vulnerability in an asset,

with impact usually measured in terms of cost to the asset's stakeholders. The sum of the products of the threats' impact and the probability of their occurring is the total risk to the information asset.

In E-healthcare system, health records are most important personal and valuable information. Maintaining security for such kind of information system is very important for maintaining confidentiality. Nowadays most of hospitals are providing best service in E-healthcare with enhanced online services. Patient can access records from their place itself, need not to carry health records are hardcopy file, Tablet details, lab reports, and scan reports. Every document is converted into digital data and maintained in a central location called server. The server will be maintained by the hospitals and one of the IT specialties will be appointed as a record manager. If new patient come for a checkup or general enquiry about him/her health then a new patient ID and other related details are collected from the patent. The records of individual patient will be maintained by the hospital and every time checkup details will be updated. The available digital records can be accessed from any were from remote place. Every hospital develops and maintains an E-health care application with enough security features. The patient can access their own records by using individual login with unique patient ID and Password. Once authentication is verified then he/she is allow to access the records. This is method of verification one of classical method and it is to attack by the known/unknown people during the insecure channel communication.

In this paper, we have proposed an efficient password authentication scheme using smart card for E-healthcare application. The proposed scheme is suitable for current and future years, because now the government makes, all the records of a common people is modernized by using smart cards. In such situation, we need an efficient security system for providing information assurance. Password based authentication schemes are classical and well studied solution for the users from different levels. In this paper, we have proposed a password based authentication scheme combined with public key cryptography.

The reaming sections of paper organized as follows, next section provides an overview about the authentication scheme with smart card applications. In this section, we have made a study about the password based authentication scheme using smart card irrespective of application. Section 3, provides details explanation of proposed authentication scheme. Section 4, provides result and discussions for the proposed scheme with related schemes. In this section, we have made a time complexity for each phase and execution time comparison with related schemes. In section 5, we have conclude the paper with remarks and future enhancements.

II. RELATED WORK

Kim et al., [1] proposed two ID-based password authentication schemes, which does not require a dictionary of passwords or verification tables, with smart card and fingerprint. Author claims that, in this schemes, users can change their passwords freely. This scheme can withstand from the message reply attack, even without synchronization clocks. The proposed two schemes [1] requires a system to authenticate each user by each user's knowledge, possession, and biometrics, and author claims that, this feature makes the proposed schemes are more reliable

Ming Chen et al, [2] proposed a three-party password authentication key exchange protocol. Author claims that, the proposed scheme secure against the stolen smart card attack. Ming Chen et al, [2] provides a security analysis to show that the protocol is still secure if sensitive information which is stored in a smart card is extracted by an attacker

Diffie and Hellman [18] established a fundamental model for key setup as known as the Diffie-Hellman key exchange and lot of researcher and research articles [3-6] are published by

using the concept of Authenticated Key Exchange (AKE) protocols. The purpose of AKE protocol is to let two communication entities to authenticate each other and establish a common session key which is used for encryption and description the following communication

Xiong Li et al, [7] proposed a communication- and computation-efficient chaotic maps-based three-party authenticated key agreement protocol without password and clock synchronization, and formally analyze the security using Burrows–Abadi–Needham logic.

Various AKE protocols require participants to keep some information as a secret, for example, a hashed value [7]. Certainly, keeping these secrets in mind may be the most secure way, but remembering it is indeed infeasible for human beings. For this reason, we need a device to store these sensitive information.

Hsiu-Lien Yeh et al, [8] proposed a secure ECC-based authentication mechanism to overcome the security flaws in the current SIP authentication procedure forms and the author claims that the proposed scheme conquers many of attacks in previous schemes.

Xin Xu et al [22] proposed a secure and efficient two-factor mutual authentication and key agreement scheme to reduce the computational cost. This scheme enables to provide the patient anonymity by employing the dynamic identity. The author claims that, compared with other related protocols, the security analysis and performance evaluation show that the proposed scheme overcomes some well-known attacks and has a better performance in the telecare medicine information system

SK Hafizul Islam et al [9] proposed devised an anonymous and provably secure two-factor authentication protocol based on ECC. Our protocol is analyzed with the random oracle model and demonstrated to be formally secured against the hardness assumption of computational Diffie-Hellman problem. The performance evaluation demonstrated that our protocol outperforms from the perspective of security, functionality and computation costs over other existing designs

Xie et al, [10] demonstrate that Farash and Attari [5] protocol cannot resist impersonation attack and off-line password guessing attack. To overcome their security weaknesses, Xie et al [10], proposed an improved chaotic maps-based 3PAKE protocol with the same advantages. Further, he applied the pi calculus-based formal verification tool ProVerif to show that the proposed 3PAKE protocol achieves authentication and security.

Farash et al. [11] showed that Yeh et al.'s [8] scheme is vulnerable to off-line password guessing attack, user impersonation attack and server impersonation attack, in the case that the smart card is stolen and the information stored in the smart card is disclosed. Farash et al [11] proposed an improved smart card-based authentication scheme which not only conquers the security weaknesses of the related schemes but also provides a reduction in computational cost. Farash et al [11] scheme provides the user anonymity and intractability, and allows a user to change his/her password without informing the remote server.

Islam et al, [22] proposed a two factor authentication protocol for TMIS using elliptic curve cryptography (ECC) to improve Xu et al.'s [23] protocol. They claimed their improved protocol to be efficient and provide all security requirements

Chaudhry et al [12] showed that Islam et al.'s [22] protocol suffers from user impersonation and server impersonation attacks. Furthermore Chaudhry et al [12] proposed an enhanced protocol and this protocol while delivering all the virtues of Islam et al.'s protocol resists all known attacks

Farash [13] pointed out that Li *et al.*'s [24] scheme is insecure against user impersonation attack. Author claims that an active adversary can easily masquerade as a legitimate user without knowing the user's secret information. To overcome the faults, Farash [13] proposed an improved authentication scheme to overcome the security weaknesses of Li *et al.*'s [24] scheme.

Zhang et al [14] pointed out that Mishra et al.'s scheme suffers from replay attacks, man-in-the-middle attacks and fails to provide perfect forward secrecy. To overcome the weaknesses of Mishra et al.'s scheme, Zhang et al [14] proposed a three-factor authenticated key agreement scheme to enable the patient to enjoy the remote healthcare services via TMIS with privacy protection.

Tseng et al. [19] proposed a novel chaotic maps-based key agreement protocol with user anonymity. They claimed that their proposed protocol could provide mutual authentication between server and users, and allow the user to anonymously interact with the server to establish a shared session key. However, in 2011, Niu et al. [20] pointed out that [19] could not ensure the user anonymity and provide perfect forward secrecy, and then proposed a trusted third party into their protocol designing.

Xue et al. [21] pointed out that the protocol of [20] is found to have several unsatisfactory drawbacks, and given some improvements to meet the original security and performance requirements. Meanwhile, [21] also overcame the security flaws of [19].

Mathematical Foundation

The proposed scheme requires some mathematical foundations and the following section explains clearly,

Collision Resistant one-way hash function

A collision-resistant one-way hash function is formally defined by [35] and following session explains,

Definition 1: A collision-resistant one-way hash function $h: \{0,1\}^* \rightarrow \{0,1\}^l$ *is a deterministic algorithm, which produces a fixed length l-bit binary string* $h(a) \in \{0,1\}^l$ *for an arbitrary length binary input string* $a \in \{0,1\}^*$. *If* $Adv_A^{HASH}(t)$ *is an adversary A's advantage in finding collision, we have*

$$Adv_A^{HASH}(t) = Pr[(a,b) \Leftarrow_R A: a \neq b \ \ and \ h(a) = h(b)]$$

where $Pr[E]$ *is the probability of an event E and* $(a,b) \Leftarrow_R A$ *is a pair* (a,b) *randomly chosen by A. Here, A is probabilistic, and its advantage is derived in execution time t over the random choice.* $h(.)$ *is collision-resistant if* $Adv_A^{HASH}(t) \leq \in_{HASH}$, *for any sufficient small* $\in_{HASH} > 0$.

III. PROPOSED SCHEME

The proposed scheme has three phase, 1) Registration phase, 2) Login and Authentication Phase, 3) Mutual Authentication Phase and 4) Password Changing Phase.

Basic Notations

Basic Notation	Meaning
U_i	User i
ID_i	Identity of User U_i
S	Server
ID_S	Identity of Server S
$r_i, r_j, n_i \; and \; m_j$	Random nonce values
PW_i	Password of User U_i
RID_i	Shadow Identity of user U_i
RPW_i	Shadow Password of user U_i
S_{Key}	Secret Key of Server S
$h(.)$	One Way Hash Function
T_S, T_C	Time Stamp
ΔT	Legal time interval between two participants communication
$\oplus$	XOR-Operator
$\|\|$	Concatenation-Operator
$E_{S_{Key}}(M)$	Symmetric Key Encryption for Message M
$D_{S_{Key}}(M)$	Symmetric Key Decryption for Message M
SK	Session Key
$P(x, y)$	Any one of the affine point from EC

1) **Registration Phase**: If a new patient comes to register with the hospital server then the following steps performed and a smart card will be issued by the hospital. The following algorithm illustrate the steps in registration phase
2) **Authentication Phase**: If the patient is registered with hospital during the previous visit then he/she can insert their card with the card reader. The following algorithm illustrate the steps for verification of user identity
3) **Mutual Authentication Phase**: Mutual authentication is one of the main part in remote authentication because to avoid reply and man-in-the-middle attack. The proposed scheme provides mutual authentication for server verification. The following algorithm illustrates the steps in mutual authentication.
4) **Password Changing Phase:** In the proposed scheme, user can change his password without the knowledge of server. The password changing is authenticated by the smartcard reader itself and password has been changed without communication cost and with minimum computational cost.

Registration Phase

User U_i	Server S
1. A User U_i can selects his identity ID_i and password PW_i freely without servers knowledge 2. Select a random nonce n_i 3. Compute $RID_i = h(ID_i \|\| n_i \|\| T_R)$ and $RPW_i = h(PW_i \|\| n_i \|\| T_R)$ 4. Send a Registration request to Server S (RID_i, RPW_i, n_i, T_R)	1. Receives the Registration request (RID_i, RPW_i, n_i, T_R) from User U_i 2. Select a random nonce m_i 3. Compute $CID_i = E_{S_{Key}}(h(RID_i \|\| ID_S \|\| m_i))$ 4. Compute $m_i.n_i.P(x,y)$ using EC arithmetic and Server S kept the copy for every registered user 5. Stores following attributes on the Smart Card SC_i $\langle RID_i, RPW_i, T_R, m_i.n_i.P(x,y), h(.), CID_i, ID_S \rangle$

Login Phase

User U_i	Server S
1. User U_i, Enters his card with the card reader 2. Enters his Identity ID_i and Password PW_i 3. Compute $RID_i^{new} = h(ID_i \|\| n_i \|\| T_R)$ and $RPW_i^{new} = h(PW_i \|\| n_i \|\| T_R)$ 4. $If\ (RID_i^{new} == RID_i\ \&\&\ RPW_i^{new} == RPW_i)\ then$ a. Accept login request and 5. Else Reject the login request 6. Select a random nonce r_i 7. Compute $r_i.m_i.n_i.P(x,y)$ (*P(x, y)* ECC-Point) 8. Compute $C_1 = r_i \oplus h(CID_i \|\| T_c \|\| m_i.n_i.P(x,y))$ and $C_2 = h(CID_i \|\| r_i.m_i.n_i.P(x,y) \|\| T_c)$ 9. Generate a login request $LR = \langle C_1, C_2, CID_i, T_c \rangle$	1. First, Check the Time validity with legal time interval, $\Delta T \leq (T_s - T_c)$ 2. If it is correct then go to the next step 3. Else Reject the login request LR 4. Compute $r_i = C_1 \oplus h(CID_i \|\| T_c \|\| m_i.n_i.P(x,y))$ 5. Compute $r_i.m_j.n_iP(x,y)$ 6. Compute

1. Receives $MA = \langle C_3, C_4, T_s \rangle$ at T_m and check the legal time interval, $\Delta T \leq (T_s - T_m)$ 2. If it is correct then accept the mutual authentication message 3. Otherwise, reject the mutual authentication and login request 4. Compute M= $h(RID_i \| \| ID_S \| \| n_i) = D_{S_{Key}}(CID_i)$ 5. Compute $r_j = C_3 \oplus M$ 6. Compute $Q(x,y) = r_j.r_i.n_i.m_j P$ *(P(x,y)* ECC-Point) 7. Compute Session key $SK = h(Q_x(x,y) \| \| T_c \| \| T_s \| \| M)$ 8. $If\ \left(CID_i = D_{SK}(C_4)\right)\ then\ accept,$ $Otherwise\ \ reject$	$C_2^{new} = h(CID_i \| \| r_i.m_j.n_i.P(x,y) \| \| T_c)$ 7. $If(C_2 == C_2^{new})\ then\ \ accept$ 8. $Otherwise,\ \ Reject\ LR$ 9. Select a random nonce r_j and 10. Compute $Q(x,y) = r_j.r_i.m_j.n_i P(x,y)$ *(P(x,y)* ECC-Point) 11. Compute $M = h(RID_i \| \| ID_S \| \| n_i) = D_{S_{Key}}(CID_i)$ 12. Compute Session key $SK = h(Q_x(x,y) \| \| T_c \| \| T_s \| \| M)$ 13. Compute $C_3 = r_j \oplus M$ and $C_4 = E_{SK}(CID_i)$ 14. Send a mutual authentication message along with $MA = \langle C_3, C_4, T_s \rangle$

Password Changing Phase

User U_i
1. A User U_i can change his password PW_i freely without servers knowledge 2. Compute $RPW_i^{new} = h(PW_i \| \| n_i \| \| T_R)$ 3. $If(RPW_i^{new} == RPW_i)\ then$ allow to change his password 5. User enter his new password PW_{new} and compute new $RPW_i^{new} = h(PW_{new} \| \| n_i \| \| T_R)$ 6. Replace RPW_i with new RPW_i^{new} on smart card SC_i

IV. SECURITY ANALYSIS

In this section, we have analyzed the security and performance of the proposed scheme and make comparisons with other related works. The security analysis is performed in two ways, formal security analysis and informal security analysis.

Formal Security Analysis

We have used Random Oracle Model (ROM) for formal security analysis and this is an famous security analysis model. A random oracle security model has a two decades history in modern cryptography and it was first formulated by Bellang and Roguway [32]. In Random Oracle (RO) model assumes the existences of a public oracle H and this will be accesses by all the users including adversary.

Security of Session Key (SK): A set of experiments are conducted by the adversary $(\mathcal{A})$ for identify the original session key between an instances of real session key and a random key (random bits). Through random oracle model (H), the A is permitted to query several test queries and the output of test query must be consistent with respect to a bit d. At the end of the experiments, adversary $(\mathcal{A})$ returns a guessed bit d', if $d' = d$, then he/she wins the game.

Let $Succ$ be the event that $\mathcal{A}$ wins the game, the advantage of $\mathcal{A}$ is to break the proposed protocol P and the probability of event occurrence is noted as $\Pr[Succ]$. The advantage of A breaking the security of proposed protocol is computed as $Adv_P^{ake} = |2.\Pr[\text{Succ}] - 1|$ protocol P is considered as a secure authentication scheme in the RO model$iff\ Adv_P^{ake} \leq \delta$, for all sufficiently small $\delta > 0$. RO model [4] is designed as follows, all the participants and adversary $(\mathcal{A})$ are provided with an one-way-hash function $h(.)$. The RO model is simulated with the hash oracle H (as mentioned above)

Theorem 1: Let $\mathcal{A}$ be an adversary mode running in a polynomial running time *t* against the proposed protocol *P* using random oracle model (ROM). Let us consider *D* be a uniformly distributed password dictionary supposed that no node is compromised by the adversary, then we have the probability of breaking the session key security of *P* by the adversary is estimated as

$$Adv_P^{ake} \leq \frac{q_h^2}{|Hash|} \leq \frac{q_{send}}{2^{l-1}.|D|} \leq 2.Adv_{G_P}^{ECDLP}(t)$$

Here, $Adv^{ECDLP}(t), q_h, |Hash|, q_{send}\ and\ |D|$ are the advantage of $\mathcal{A}$ of breaking the ECDLP over GF(p) with respect to EC-equation, the number of Hash queries made, the range space of the hash function, the number of hash query send to RO, and the size of *D*, respectively.

Proof: we define a sequence of games $G_i,\ i = 0,1,2,3, and\ 4$ and we have a $Succ_i$bit to denote the event of adversary success in the guessing process in game G_i. The conclusion of the proof is to prove that the adversary $\mathcal{A}$ has negligible amount of advantage to break the session key security of *P*.

Game G_0: The game $G_0$is the real attack by the adversary $\mathcal{A}$ against the proposed protocol *P* in random oracle model. At the beginning of this game, the bit *b* is chosen at random by definition, we have

$$Adv_P^{ake}(A) = 2Pr[Succ_0] - 1 \qquad (1)$$

Game G_1: This game simulated by the adversary $\mathcal{A}$ as eavesdropping attacks by querying $Execute(\pi^t, \pi^l)$ to oracle. The output of the $Execute(\pi^t, \pi^l)$ query is compare by the adversary using Test oracle, this query will decide whether the output of the text is the real session key or a random number. The proposed protocol P computes the session key$SK' = h(Q_x(x,y)||T_c||T_s||M)$, here $Q_x(x,y) = r_j.r_i.n_i.P(x,y)$ is new and fresh for every new session and time stamp (T_c, T_s) introduce the freshness for the login request and session key. The game G_1will not provide success result to the adversary $(\mathcal{A})$, because of two arguments, given below,

Argument 1: A forged session key (SK') can be generated $iff\ Q_x(x,y)$ is known by the adversary$(\mathcal{A})$. The values of $P(x,y), EC-equation\ and\ p$ are publicly available to all the participants including adversary $\mathcal{A}$ according to Random Oracle Model. Even though, the adversary $\mathcal{A}$ cannot reproduce the original session key SK, without knowing the values of $r_j, r_i,\ and\ n_i$. Here $r_j\ and\ r_i$ are the two random variables newly created for every new login session, n_i is unique random value created during the registration session itself. According to the argument, the adversary cannot create forged session key (SK')

Argument 2: The adversary $\mathcal{A}$ make an attempt to find the $M$from the login request (LR). This is not possible because of the secret key (S_{key}) is maintained by the server $(\mathcal{S})$

The probability of success will not increase for adversary $(\mathcal{A})$ for the gameG_1. Then, $G_1$is equivalent to G_0 and the corresponding probability are equal

$$\Pr[Succ_0] = \Pr[Succ_1] \quad (2)$$

Game G_2: This game is different from $G_1$and we add the simulations of the Send and the Hash oracles. This game models an active attack in which the adversary $\mathcal{A}$ tries to swindle a participant into accepting a message fabricated by it. $\mathcal{A}$ queries the Hash oracle repeatedly to find collisions. Note that the login request $LR = \langle C_1, C_2, CID_i, T_c \rangle$ and $MA = \langle C_3, C_4, T_s \rangle$ are the two messages capture by the adversary. Both the messages are associate with the $random\ r_i\ and\ r_j, Secret\ key\ S_{Key}\ and\ n_i.m_jP(x,y)$. Here $r_i\ and\ r_j$ are random numbers, therefore no collisions will occur if $\mathcal{A}$ queries to the Send oracle. By using the birthday paradox [46], we get

$$|\Pr[Succ_1] - \Pr[Succ_2]| \leq \frac{q_h^2}{2.|Hash|} \quad (3)$$

Game G_3: This game G_3simulates the CorruptSC oracle and models the smartcard loss attack. If the password has low-entropy, the adversary might try online dictionary attack with the information obtained from the smart card. The adversary extracts the RPW_i value from SC_i, but original password PW_i could not be extracted or derived, due to collision resistant hash function even by the known values of $n_i\ and\ T_R$. If the number of wrong password input or login should be limited by the system, probability can be estimated as

$$|\Pr[Succ_2] - \Pr[Succ_3]| \leq \frac{q_{Send}}{2^l.|D|} \quad (4)$$

Game G_4: This game models an attack wherein the adversary has compromised the server and he/she has the smart card SC_i of legal user U_i by using CorruptSC oracle. Thus, A can extract and use the $n_i.P(x,y)$ value from theSC_i. The proposed protocol P generates the SK by using $Q(x,y) = r_j.r_i.n_i.m_j.P(x,y)$ two random nonce r_j *and* r_i are user for $Q(x,y)$ point calculation. Let $Adv_{G_P}^{ECDLP}$be the advantage of the adversary in the experiment wherein A has to distinguish between $r_j.r_i.n_i.m_j.P(x,y)$ and a random numbers given $r_i.n_i.m_j.P(x,y)$ and$r_j.n_i.m_j.P(x,y)$. In addition to that, session key $SK = h(Q_x(x,y)||T_c||T_s||M)$ is generated using $Q_x(x,y)$ and $M = h\left(RID_i\middle||ID_S\middle||m_j\right)$ are unknown value and T_c *and* T_s are known to adversary. The adversary needs to derive the r_j, r_i, n_i *and* m_j for EC-point calculation $Q(x,y)$ and he/she needs to know $RID_i = h(ID_i||b_i||T_R)$, ID_S and m_j for calculating $M = h\left(RID_i\middle||ID_S\middle||m_j\right)$, respectively. We then have

$$|\Pr[Succ_3] - \Pr[Succ_4]| \leq Adv_{G_P}^{ECDLP}(t) \quad (5)$$

According to the last Game G_4, it is clear that $\Pr[Succ_4] = \frac{1}{2}$. Thus, from the equations (1) to (5), we have

$$\left|\Pr[Succ_0] - \frac{1}{2}\right| \leq \frac{q_h^2}{2.|Hash|} + \frac{q_{send}}{|D|} + Adv_{G_P}^{ECDLP}(t) \quad (6)$$

$$\Pr[Succ_0] = \frac{Adv_P^{ake}(A)}{2} + \frac{1}{2} \quad (7)$$

Hence, by solving the equations (6) and (7), we have

$$Adv_P^{ake}(\mathcal{A}) \leq \frac{q_h^2}{|Hash|} + \frac{2.q_{send}}{|D|} + 2.Adv_{G_P}^{ECDLP}(t) \quad (8)$$

The corruptSC oracle in Game G_4simulates the attacks when a smart card is steal by someone (assume that adversary $\mathcal{A}$). In this game, $Adv_P^{ake}(\mathcal{A})$ is highly probable and this situation protocol P is secure under the assumption of Elliptic Curve Discrete Logarithm Problem (ECDLP) is computationally infeasible for a probabilistic polynomial time adversary $(\mathcal{A})$. The session key $SK = h(Q_x(x,y)||T_c||T_s||M)$ is secure based on ECDLP even when leaking of sensitive information from the smart cards (corruptSC). Thus, the proposed protocol is secure and maintains the perfect forward secrecy authentication.

V. PERFORMANCE ANALYSIS

In this subsection, we evaluate the runtime analysis of our proposed scheme in terms of computational cost. Table compares the computational cost of our proposed scheme with related schemes using cryptographic algorithms. We have made two comparisons first for phase wise analysis and the second one for cryptographic algorithm wise analysis. We have used simple notation for time-consuming operations, such as modulus exponential operations, symmetric encryption/decryption operations, asymmetric encryption/decryption operations and hashing.

The proposed scheme is compared with the related schemes of Xu et al. [22], Amin-Biswas [24], Amin et al. [28], Lu et al [30], Amin et al [33] and Mohammad Wazid et al [34] with respect to computational cost, communication cost during login and authentication and key agreement phases. We have not taken the computational cost and communication cost measurement for registration phase and password changing phase, because these phases are not frequently performed operations of the protocol.

The following table 2 and figure 1 compares the computation cost of our scheme with respect to the related schemes. The following notation are used for easy understanding and the corresponding experiment values are reported in [61], [62], [19] and [34]. In [19], it is assumed that $T_{BH} = T_{fe} \approx T_{ecm}$

Notation	Meaning	Experiment value in Sec
T_{ecm}	ECC point multiplication	0.063075s
T_{eca}	ECC point addition	0.010875s
$T_{E/D}$	Encryption/Decryption using symmetric cryptosystem (AES)	0.0087s
T_H	Hash function	0.0005s
T_{BH}	A biohashing operation	0.063075s
T_{fe}	A fuzzy extraction operation	0.063075s

Table 1: Execution Time for Cryptographic Operations

Schemes	Login Phase	Authentication and Key agreement Phase	Total Cost	Total Cost in sec
Xu et al [22]	$3T_H + 2T_{ecm}$	$8T_H + 3T_{ecm}$	$11T_H + 6T_{ecm}$	$\approx 383.95ms$
Amin-Biswas [24]	$1T_{BH} + 3T_H + T_{ecm}$	$2T_{E/D} + 2T_{eca} + 7T_H + 4T_{ecm}$	$2T_{E/D} + 2T_{eca} + 10T_H + 5T_{ecm} + 1T_{BH}$	$\approx 422.60ms$
Amin et al [28]	$1T_{BH} + T_D + 2T_H + 2T_{ecm} + T_{eca}$	$2T_{E/D} + 6T_H + 4T_{ecm} + 3T_{eca}$	$1T_{BH} + 3T_{E/D} + 8T_H + 6T_{ecm} + 4T_{eca}$	$\approx 515.13ms$
Lu et al [30]	$1T_{BH} + 3T_H + T_{ecm}$	$6T_H + 3T_{ecm}$	$1T_{BH} + 9T_H + 4T_{ecm}$	$\approx 319.88ms$
Amin et al [33]	$5T_H + 3T_{ecm}$	$4T_{E/D} + 11T_H + 8T_{ecm}$	$4T_{E/D} + 16T_H + 11T_{ecm}$	$\approx 736.63ms$
Mohammad Wazid et al [34]	$1T_{fe} + 7T_H + 1T_{ecm}$	$2T_{E/D} + 7T_H + 2T_{ecm} + 2T_{eca}$	$2T_{E/D} + 14T_H + 3T_{ecm} + 2T_{eca} + 1T_{fe}$	$\approx 298.45ms$
Proposed Scheme	$4T_H + 1T_{ecm}$	$3T_H + 2T_{ecm} + 2T_{E/D}$	$7T_H + 3T_{ecm} + 2T_{E/D}$	$\approx 210.125ms$

Table 2: Runtime Analysis

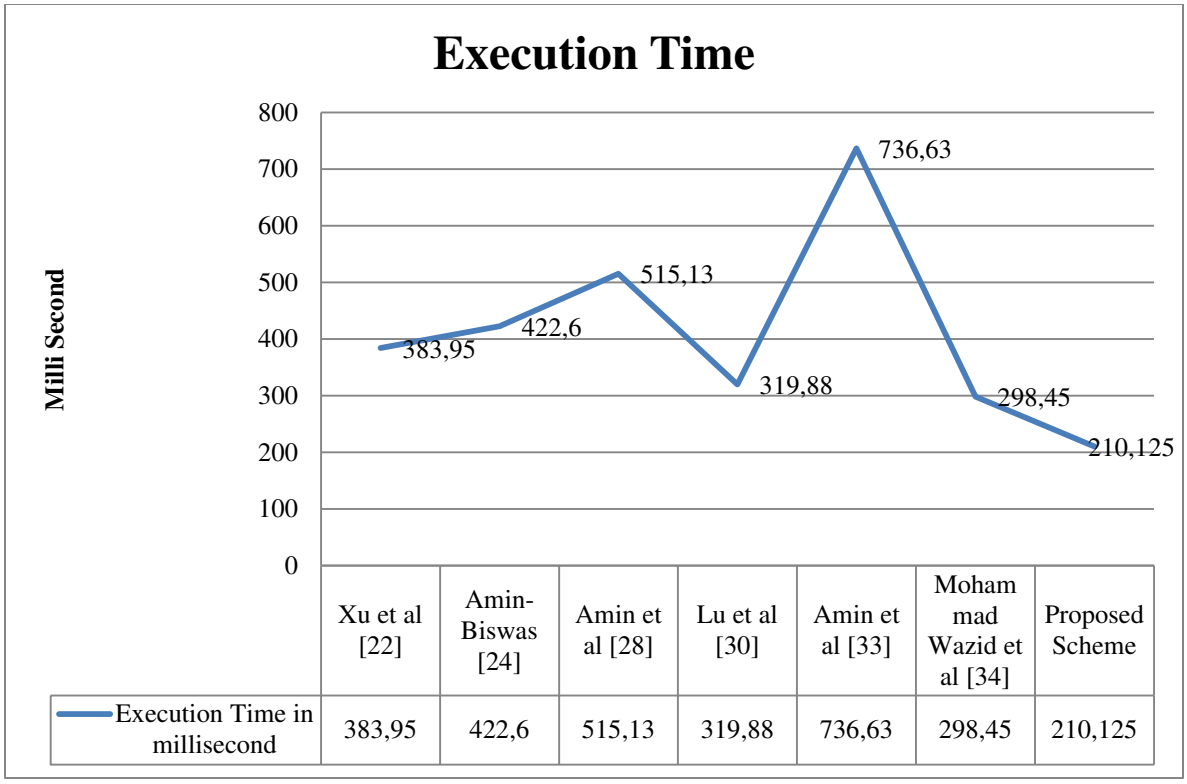

Figure 1: Execution Time comparison with related schemes

The communication cost of the proposed scheme is compared with other related schemes given in table 3. We have compare with reasonable assumption that ID_ihas 160 bits length, prime number p in $E_p(a,b)$is of 160-bits (it is equivalent to 1024-bits RSA security [63]) and random nonce are of 128-bits. The time stamp is 32-bits and symmetric encryption/decryption is of 128-bits (here we have used AES-128 symmetric encryption algorithm). We have consider a standard SHA-1 as a hash function and the message digest size of 160-bits [64]. We have compared the proposed scheme with these values as a communication overhead. Note that the proposed scheme, during the login phase, $LR = \langle C_1, C_2, CID_i, T_c \rangle$ needs $LR = \langle C_1 = 160, C_2 = 160, CID_i = 128, T_c = 32 \rangle = (160 + 160 + 128 + 32) = 480$bits, during the authentication and key agreement phase we needs $MA = \langle C_3 = 160, C_4 = 128, T_s = 32 \rangle = (160 + 128 + 32) = 320$bits. The total cost for the proposed scheme is $(480 + 320) = 800$ bits. As a result, the proposed scheme requires minimum communication cost 800 bits compared all other related schemes.

Schemes	Total No. of messages	Total bits
Xu et al [22]	2	1184
Amin-Biswas [24]	3	1728
Amin et al [28]	3	1888
Lu et al [30]	3	1376
Amin et al [33]	4	2688
Mohammad Wazid et al [34]	2	1760
Proposed Scheme	2	800

Table 3: Comparison of the communication cost

VI. CONCLUSION

E-healthcare system maintains the user/patient sensitive information in a common place and these information systems are subject to attack. Most of the information systems are fails to provide effective authentication for remote access. In this paper, we have proposed an efficient password based authentication scheme using smart card with Elliptic Curve Cryptography. The proposed scheme is a two factor authentication scheme combined with smart card and password. This scheme is more secure, because we are using ECC for session key generation and this session key is used for mutual authentication symmetric key cryptography. The proposed scheme is verified with the Random Oracle Model (ROM) for real time security proof. The proposed scheme is highly secure under ROM. The proposed scheme is requires nominal amount of computational cost and communication cost compare to other related schemes.

REFERENCE

[1] Hyun-Sung Kim, Sung-Woon Lee and Kee-Young Yoo, "ID-based password authentication scheme using smart cards and fingerprints," ACM SIGOPS Operating Systems Review, Volume 37 Issue 4, 2003 Pages 32-41

[2] Chien-Ming Chen, Linlin Xu, Weicheng Fang, Tsu-Yang Wu, "A Three-Party Password Authenticated Key Exchange Protocol Resistant to Stolen Smart Card Attacks,"Advances in Intelligent Information Hiding and Multimedia Signal Processing, 2016 pp 331-336

[3] Chen, C.M., Wang, K.H., Wu, T.Y., Pan, J.S., Sun, H.M., "A scalable transitive human-verifiable authentication protocol for mobile devices," IEEE Transactions on Information Forensics and Security, 2013, Vol. 8, No.8, pp. 1318–1330

[4] Sun, H.M., He, B.Z., Chen, C.M., Wu, T.Y., Lin, C.H., Wang, H. "A provable authenticated group key agreement protocol for mobile environment," Information Sciences Vol. 321, pp.224–237, 2015

[5] Farash, M.S., Attari, M.A. "An enhanced and secure three-party password-based authenticated key exchange protocol without using servers public-keys and symmetric cryptosystems," Information Technology and Control Vol. 43, No.2, pp. 143–150, 2014

[6] Gope, P., Hwang, T. "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks," Journal of Network and Computer Applications, Vol. 62, pp. 1–8, 2016

[7] Li, X., Niu, J., Kumari, S., Khan, M.K., Liao, J., Liang, W. "Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol," Nonlinear Dynamics, Vol. 80, No.3, pp. 1209–1220, 2015

[8] Yeh, H.L., Chen, T.H., Shih, W.K., "Robust smart card secured authentication scheme on sip using elliptic curve cryptography," Computer Standards & Interfaces, Vol. 36, No.2, pp. 397–402, 2014

[9] Islam, S.H., Khan, M.K., "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," Journal of medical systems, Vol.38, No. 10, pp. 1–16, 2014

[10] Xie, Q., Hu, B.,Wu, T. "Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using servers public key and smart card," Nonlinear Dynamics, Vol. 79, No.4, pp. 2345–2358, 2015

[11] Farash, M.S., Kumari, S., Bakhtiari, M. "Cryptanalysis and improvement of a robust smart card secured authentication scheme on sip using elliptic curve cryptography," Multimedia Tools and Applications, Vol. 75, No.8, pp. 4485–4504, 2016

[12] Chaudhry, S.A., Naqvi, H., Shon, T., Sher, M., Farash, M.S. "Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems," Journal of Medical Systems, Vol. 39, No. 6, pp. 1–11, 2015
[13] Farash, M.S., "Cryptanalysis and improvement of an improved authentication with key agreement scheme on elliptic curve cryptosystem for global mobility networks," International Journal of Network Management, Vol. 25, No.1, pp. 31–51, 2015
[14] Zhang, L., Zhu, S., Tang, S., "Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme," IEEE Journal of Biomedical and Health Informatics, 2017
[15] Zhao, F., Gong, P., Li, S., Li, M., Li, P., "Cryptanalysis and improvement of a three-party key agreement protocol using enhanced chebyshev polynomials," Nonlinear Dynamics, Vol. 74, No. 1-2, pp. 419–427, 2013
[16] Chen, C.M., Xu, L., Wu, T.Y., Li, C.R., "On the security of a chaotic maps-based three-party authenticated key agreement protocol," Journal of Network Intelligence, Vol. 2, pp. 61–65, 2016
[17] Diffie, W., Hellman, M., "New directions in cryptography," IEEE transactions on Information Theory, Vol. 22, No.6, pp. 644–654, 1976
[18] H.R. Tseng, R.H. Jan, and W. Yang, "A chaotic maps-based key agreement protocol that preserves user anonymity," IEEE International Conference on Communications, ICC09, Dresden, Germany, pp. 1-6, 2009.
[19] Y.J. Niu, X.Y. Wang, "An anonymous key agreement protocol based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol.16, no. 4, pp. 1986-1992, 2011
[20] K.P. Xue, P.L. Hong, "Security improvement on an anonymous key agreement protocol based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol.17, no. 7, pp. 2969-2977, 2012
[21] Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., and He, L., A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *J. Med. Syst.* 38:9994, 2014
[22] Irshad, A., Sher, M., Faisal, M.S., Ghani, A., Ul Hassan, M., Ch, S.A., "A secure authentication scheme for session initiation protocol by using ECC on the basis of the tang and liu scheme," *Secur. Comm. Netw.*, 2013
[23] Wu, S., and Chen, K., "An efficient key-management scheme for hierarchical access control in e-medicine system," *J. Med. Syst.* Vol. 36, No.4. pp. 2325–2337, 2012
[24] Li X, Wen Q, Zhang H, Jin Z. "An improved authentication with key agreement scheme on elliptic curve cryptosystem for global mobility networks," International Journal of Network Management, 2013, Volume 23 Issue 5: pp.311-324
[25] Lai, H., Xiao, J., Li, L., Yang, Y., "Applying semigroup property of enhanced chebyshev polynomials to anonymous authentication protocol," Mathematical Problems in Engineering, 2012
[26] B. L. Chen, W. C. Kuo and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme," International Journal of Communication Systems, in press. (http://dx.doi.org/10.1002/dac.2368)
[27] W. S. Juang, S. T. Chen and H. T. Liaw, "Robust and efficient password-authenticated key agreement using smart card," IEEE Transactions on Industrial Electronics, vol. 55, no. 6, pp. 2551-2556, 2008
[28] X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," Journal of Network and Computer Applications, in press. (http://dx.doi.org/10.1016/j.jnca.2013.02.034.)

[29] R. Song, “Advanced smart card based password authentication protocol,” Computer Standards and Interfaces, vol. 32, no. 5, pp. 321-325, 2010.
[30] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang, and Z. Y. Feng, “Improvements of juang et al.'s password-authenticated key agreement scheme using smart cards,” IEEE Transactions on Industrial Electronics, vol. 56, no. 6, pp. 2284-2291, 2009
[31] X. X. Li, W. D. Qiu, D. Zheng, K. F. Chen, and J. H. Li, “Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards,” IEEE Transactions on Industrial Electronics, vol. 57, no. 2, pp. 793-800, 2010
[32] Bellare M, Rogaway P (1994) Entity authentication and key distribution. In: CRYPTO 93 Advances in Cryptology. Springer, pp 232–249
[33] V. Shoup, Sequences of Games: A Tool for Taming Complexity in Security Proofs, 2005. [Online]. Available: http://www.shoup.net
[34] T. F. Lee and T. Hwang, “Provably secure and efficient authentication techniques for the global mobility network,” *J. Syst. Softw.*, vol. 84, no. 10, pp. 1717–1725, Oct. 2011
[35] D. Brown, Generic groups, collision resistance, and ECDSA, Designs, Codes and Cryptography, 35 (2005), pp. 119-152