International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

Image based ECC Mutual Authentication Scheme for Cloud Assisted TMIS

Syed Amma Sheik[1], Saleem Durai[2]
[1] Research Scholar, School of Computer Science and Engineering, Vellore Institute of Technology, Tamil Nadu, India.
[2] Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Tamil Nadu, India.
[2]Corresponding Author: masaleemdurai@vit.ac.in

Abstract - In this modern era, cloud-based services like e-commerce, e-gate, and so on provide immense services to humans. Healthcare centers are gradually moving to cloud-based services. In which, both the hospital and patients are connected remotely online and patient gets treatment quickly. Increasing the demand in Telecare Medical Information System (TMIS) needs to ensure the security and privacy of the healthcare centers and patients' information. In this paper, we have proposed an efficient and provably secure Elliptic Curve cryptography image based mutual authentication scheme for cloud assisted TMIS. The proposed authentication schemes ensure the secured treatment provided to patients from healthcare center through online. The patient can upload their health condition data to cloud via mobile device for the treatment. The proposed authentication scheme required minimum computational cost with minimum communication overhead. The proposed authentication scheme preserves patient anonymity and withstands the known and chosen plaintext attack. The security analysis for the proposed scheme shows that the proposed authentication scheme is more secure. It shows that the proposed authentication scheme is performing well compare to the related authentication schemes.

Keywords - Authentication, Cloud Environment, Elliptic Curve Cryptography (ECC), Image based, Patient anonymity.

1. Introduction

TMIS provide remote online services to patient without visiting the hospital. Patient healthcare assessed reports or patient data can easily be transferred from one hospital to another via cloud environment without the duplication of patient data. Cloud platforms connect the hospital doctors, patient and healthcare centers. The authentication is vital part for the cloud assisted TMIS to provide the secure communication between cloud server and users like patients, doctor and hospital centers. The set of rules validate the authentication process between the user and server. The facial id along with password or smart card is an important user id for remote authentication. A lot of researches have been taken place for the past two decades in the area of authentication schemes includes password, smart card and biometric based. Fig. 1 illustrates the entire process of remote facial authentication and message communication between users and cloud server.

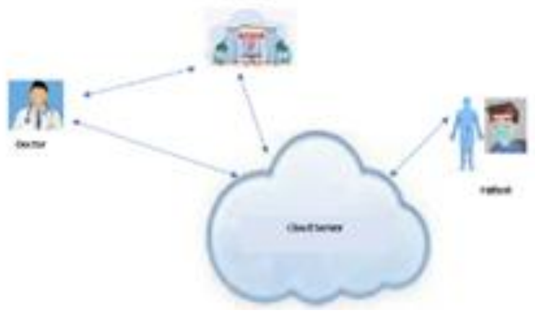

Fig 1:Facial ID based authentication

In Fig.1, depicts that users and cloud servers communicate through public channel. All the message communications carried out between the users and cloud server through facial id of the users. Then, this id will be encrypted and decrypted by ECC via public channel. This proposed method ensures that both the legal parties are communicating each other's through unlocking the challenge messages mutually send and received by both the parties.

In any authentication process there will be three parties involved. The first party is the users or clients, second party is the server and third party is the adversary. So, the adversary will try to steal the authentication information from the users and server. In this scheme as mentioned earlier the legality of the users and server ensured through mutual authentication established through ECC.

This scheme ensures that the challenges from adversary are addressed and it is proved as secure authentication scheme using users face id.

1.1 Contribution

In this paper, we have proposed a image based mutual authentication scheme for cloud assisted TMIS. In this scheme, we have used facial id to authenticate the message communication process. we have compared and referred many recently published papers.

1.2 Organization of the Paper:

The organization of remaining sections of the paper as follows, the section 2 provides a wide survey on two factors, three factor and image-based authentication schemes. In the section 3, we have described about the proposed authentication scheme. The section 4 explains about the security analysis for the proposed authentication scheme. Section 5 provides the performance analysis for the proposed authentication scheme, which explains the computational cost analysis. In the Section 6, we conclude our proposed scheme with remarks.

2. Related Work

In 1981, Lamport [12] introduced remote authentication system using overhead hash functions and verification table. This system considered as pioneer of authentication system. Researchers had focused authentication scheme and proposed their work [13,14,15,16] due to the pioneer version of Lamport system. In 2000, Hwang et al. [17] proposed authentication scheme using smart cards without a password verifier table. However, this scheme is not providing password updating phase.

In 2015, Amin et.al. [7] proposed a smartcard-based user authentication and key agreement protocol for TMIS. This proposed method illustrated the multi user and services accessing the medical servers. The patient can have direct communication to the doctor. They proved that it withstands for security attacks. The digital signatures and image based accessed not mention in the proposed method. In addition to this, several smart card based authentication schemes were proposed by researchers[18-23].

In 2016, Chaudhry SA et. al [6] proposed a biometric authentication scheme for TMIS using Elliptic Curve Cryptography for multi servers. This scheme improved Amin et al [7] scheme by withstanding stolen smartcard, stolen verifier attacks and scalability issues of the password change phases.

In 2017, Mohit et.al. [3] proposed a standard mutual authentication protocol for cloud-based healthcare system. They emphasis that proposed method is light weight mutual authentication protocol and secured against patient anonymity and stolen mobile attacks.

In 2018, Kumar V. et.al [8] proposed a mutual authentication framework for TMIS as an improved version of Mohit.et.al [3] scheme. It enhances the security flaws of Mohit et. al [3] scheme such as security verifier attack, patient anonymity, impersonation attack and session key agreements.

In 2018, Li et al [1] proposed a cloud assisted mutual authentication and privacy preservation protocol for cloud based TMIS. They claimed that the proposed scheme withstands against the flaws of Mohit.et.al [3] scheme. The scheme enhanced the patient anonymity and patients unlinkablility.

In 2019, Vinod Kumar et.at al [4] proposed a secure elliptic curve cryptography based mutual authentication protocol for cloud assisted TMIS. This scheme proposed an improvement for Li. et. al. [1] schemes. It's overcome the flaws of Li.et.al scheme. The proposed scheme withstands against the man-in-the-middle attack, patient anonymity, replay attack, session key security and patient unlinkability.

In 2019, Chandrakar. P et. al [9] proposed a cloud-based authentication for health care system. In this proposed method patients directly receiving the medical facilities from the doctor through mobiles. The user privacy and reliability of the system shown and it is compared with other existing proposed methods.

In 2020, V.Suresh Kumar et. al [2] proposed a chaotic map based mutual authentication and key agreement protocol for TMIS. The proposed scheme withstands for insider attack, stolen password attacks, preserves user anonymity and mutual authentication. However, user facial id has not been discussed in the proposed scheme.

In 2021, Rehman S et. al [11] proposed a hybrid scheme with an implementation of both ECC and AES algorithm to secure authentication and data integrity for data sharing in the cloud environment. In this scheme, input file is encrypted and decrypted through proposed scheme. The authentication for different phases and security analysis were not compared. The author describes the general time consumption for various algorithms and proposed.

In 2022, Habek et. al. [10] reviewed an image-based encryption and decryption using ECC algorithm. There are 21 papers reviewed and explained about the various technology combined with ECC algorithm. The author emphasis the importance of image-based algorithm with hybrid approaches using ECC algorithm. The paper described performance analysis related with image based crypto analysis such as known plaintext attack and ciphertext only attack etc.

3. Proposed Scheme

This scheme has four main phases such as hospital center data load phase, Patient data load phase, Patient treatment phase and Patient check-up phase. The notations used throughout this paper are defined in the Table 1.

Table 1: Basic Notations

Basic Notation	Meaning
$\mathbf{P_R}$	Registered Patient
$\mathbf{H_c}$	Hospital/Healthcare Center
$\mathbf{C_e}$	Cloud Environment
$\mathbf{p_{rh}}$	Patient's report from Hospital
$\mathbf{F_{PID}}$	Facial ID of the Patients
$\mathbf{U_{HID}}$	Unique Hospital ID
$\mathbf{SK_{hc}}$	Session Key of the healthcare center
MID	Dynamically generated pseudo number
$\mathbf{Sign_{HC}}$	Signature of the healthcare center

Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

$\mathbf{SK_{PR}}$	Session Key of the Registered patient
$\mathbf{V_{PU_{HC}}}$	Verified Key of the healthcare Center
$\mathbf{Sign_{PR}}$	Signature of the Registered patient
$\mathbf{Z_q}^*$	Additive group of order q
q	The large prime
HD	Hospital Doctor
$\boldsymbol{G}$	Elliptic curve group under addition
$\boldsymbol{g}$	Base point of G
||	The string concatenation operation
⊕	The bitwise XOR operation
$\boldsymbol{h}(.)$	One way hash function
$\mathbf{E_k(M)}$	Encryption of Message M using key *k*
$\mathbf{D_k(M)}$	Decryption of Message M using key *k*
$\mathbf{s_{qi}}$	Sequence number of *i*th participants
E	Adversary

3.1. Hospital Center Data Load Phase (HDLP)

If P_R (Registered Patient) wants to upload the his/her details into Hospital Center H_c, H_c mutually authenticated with C_e and upload the patient information into C_e . The detailed steps of this phase are as follows.

1. H_c generates patient inspection report using patient face id along with patient health data $p_{rh} = (F_{PID}, D_P)$,random number $h \in Z_q{}^*$ input hospital unique identity U_{HID} and h. Then, sends message $M_{H1} = \langle U_{HID}, h, T_{hc1} \rangle$ to C_e via secure channel.

2. Upon receiving hospital request C_e verifies time stamp between hospital and cloud $T_{ce1} - T_{hc1} \leq \Delta T$, then generates random number $k \in Z_q{}^*$,computes $S_1 = h(U_{HID} \parallel h \parallel k \parallel T_{hc1})$, $K_1 = h(U_{HID} \parallel h \parallel T_{hc1})$, $E_1 = E_{K_1}(k, k', S_1, T_{ce2})$ and send message $M_{C1} = \langle E_1, T_{ce2} \rangle$to H_c via insecure communication channel.

3. Upon receiving cloud request H_c verifies time stamp between hospital and cloud $T_{hc2} - T_{ce2} \leq \Delta T$, if not satisfies, H_c terminates the session. If satisfies,

$K_1{}' = h(U_{HID} \parallel h \parallel T_{hc1})$, and decrypts (k, S_1, T_{ce2}) =$D_{K'_1}(E_1)$,computes $S_1{}' = h(U_{HID} \parallel h \parallel k \parallel T_{hc1})$

Further, H_c checks $S_1{}' equals\ S_1$,if not equal H_c terminates the session, if equals H_c authenticate the C_e.Then computes session key $SK_{hc} = h(U_{HID} \parallel S_1{}' \parallel hkg \parallel T_{ce1})$, $K_2 = h(F_{PID} \parallel U_{HID} \parallel MID)$, and encrypts $C_{HC} = E_{K_2}(p_{rh})$, then H_c produce digital signature $Sign_{HC} = S_{PRH}(h(p_{rh}))$, $S_2 = h(SK_{hc} \parallel C_{HC} \parallel Sign_{HC} \parallel T_{hc3})$, encrypts $E_2 = E_{SK_{HC}}(F_{PID}, MID, C_{HC}, S_2, Sign_{HC}, T_{ce3})$ and sends message $M_{H2} = \langle E_2, T_{hc3} \rangle$.

4. Upon receiving hospital request C_e verifies time stamp between hospital and cloud $T_{ce3} - T_{hc3} \leq \Delta T$, and computes $SK_{ceh} = h(U_{HID} \parallel S_1 \parallel hkg \parallel T_{ce1})$, the decrypts message $(F_{PID}, MID, C_{HC}, S_2, Sign_{HC}, T_{ce3}) = D_{SK_{HC}}(E_2)$, and computes $S_2{}' = h(SK_{ceh} \parallel C_{HC} \parallel Sign_{HC} \parallel T_{hc3})$ then verifies $S_2{}' equals\, S_2$, if equals C_e authenticate H_c and store patient record $F_{PID}, MID, C_{HC}, Sign_{HC}$. If not equal, it terminates the session.

3.2. Patient Data Upload phase (PDLP):

In this phase, registered patient P_R acquiring his/her health fitness data using body sensor through secured mobile devices and communicating cloud environment C_e via secured communication channel. Then, P_R and C_e mutually authenticated as follows:

1. P_R sends his/her F_{PID}, MID and send message $M_{P1} = \langle F_{PID}, MID, T_{P1} \rangle$ to C_e via secured communication channel.

2. Upon receiving hospital request C_e verifies time stamp between hospital and cloud $T_{ce4} - T_{P1} \leq \Delta T$,if it is ok, then computes $I = s_{qi} \oplus h(MID \parallel F_{PID})$then, generates random number $l \in Z_q{}^*$,computes $S_3 = h(MID \parallel F_{PID} \parallel C_{HC} \parallel Sign_{HC} \parallel l \parallel T_{ce5})$, encrypts$E_3 = E_{sq_i}(Sign_{HC},\ C_{HC},\ S_3, U_{HID}, l,\ T_{ce5})$ and send message $M_{C2} = \langle E_3, T_{ce5} \rangle$to P_R via insecure communication channel.

3. Upon receiving cloud request P_R verifies time stamp between hospital and cloud $T_{P2} - T_{ce5} \leq \Delta T$, if not satisfies, P_R terminates the session. If satisfies, $P_R$computes $N = I \oplus h(MID \parallel F_{PID})$and decrypts $Sign_{HC},\ C_{HC},\ S_3, U_{HID}, l,\ T_{ce5})$ =$D_Y(E_3)$,computes $S_3{}' = h(MID \parallel Y \parallel C_{HC} \parallel Sign_{HC} \parallel l \parallel T_{ce5})$

Further, P_R checks $S_3{}' equals\ S_3$,if not equal P_R terminates the session, if equals P_R authenticate the C_e.Then , generates random number $n \in Z_q{}^*$,further, $P_R$computes session key $SK_{PR} = h(F_{PID} \parallel U_{HID} \parallel C_{HC} \parallel S_3{}' \parallel lng \parallel T_{ce5})$, $K_3 = h(F_{PID} \parallel U_{HID} \parallel MID)$, and decrypts $p_{rh}{}^* = D_{K_3}(C_{HC})$ and checks $p_{rh}{}^*$=p_{rh}. Moreover, P_R verifies $V_{PU_{HC}}(Sign_{HC}) =$ h($p_{rh)}$ holds or not. If holds P_R computes $K_4 = h(F_{PID} \parallel HD_{ID} \parallel N)$, encrypts $C_{PR} = E_{K_4}(p_{rh}, p_{rb})$, then P_R produce digital signature $Sign_{PR} = S_{PRb}(h(p_{rb}))$, $S_4 = h(SK_{PR} \parallel C_{PR} \parallel Sign_{PR} \parallel S_3{}' \parallel lng \parallel T_{PR3})$, encrypts $E_4 = E_N(n, S_4, Sign_{PR}, C_{PR}, T_{P3})$ and sends message $M_{P2} = \langle E_4, T_{P3} \rangle$.

4. Upon receiving patient request C_e verifies time stamp between hospital and cloud $T_{ce6} - T_{P3} \leq \Delta T$, if it is does, decrypts message $(n, S_4, Sign_{PR}, C_{PR}, T_{P3}) = D_{sq_i}(E_4)$, and computes $SK_{ce} = h(F_{PID} \parallel U_{HID} \parallel C_{HC} \parallel S_3 \parallel T_{ce5})$ then

compute hash value $S_4{}' = h(SK_{PR} \parallel C_{PR} \parallel Sign_{PR} \parallel S_3 \parallel lng \parallel T_{PR3})$,verifies $S_4{}' equals\, S_{42}$, if equals C_e authenticate P_R and store patient record $F_{PID}, C_{PR}, Sign_{PR}$. If not equal, it terminates the session.

3.3. Patient Treatment Phase (PTP)

In this phase, Hospital Doctors HD and C_e mutually authenticated, and HD provides treatment to P_R. The details as follows:

1. HD sends HD_{ID}, p_{rd} and generates random number $r \in Z_q{}^*$,send message $M_{D1} = \langle HD_{ID}, r, T_{D1}\rangle$ to C_e via secured communication channel. Upon receiving hospital request C_e verifies time stamp between hospital and cloud $T_{ce7} - T_{D1} \leq \Delta T$,if it is ok, then computes $J = s_{qi} \oplus h(HD_{ID} \parallel \text{r})$then, generates random number $b \in Z_q{}^*$,computes $S_5 = h(F_{PID} \parallel HD_{ID} \parallel Sign_{HC} \parallel Sign_{PR} \parallel C_{PR} \parallel T_{ce8})$, encrypts$E_5 = E_{sq_i}(Sign_{PR}, Sign_{HC}, \text{ MID}, C_{PR}, F_{PID}, S_5, b, T_{ce5})$ and send message $M_{c3} = \langle E_5, J, T_{ce8}\rangle$ to HD via insecure communication channel.

2. Upon receiving cloud request HD verifies time stamp between hospital and cloud $T_{D2} - T_{ce8} \leq \Delta T$, if not satisfies, HD terminates the session. If satisfies, HDcomputes $Z = J \oplus h(HD_{ID} \parallel r)$and decrypts $Sign_{PR}, Sign_{HC}, \text{ MID}, C_{PR}, F_{PID}, S_5, b, T_{ce5})$ =$D_Z(E_5)$,computes $S_5{}' = h(F_{PID} \parallel HD_{ID} \parallel Sign_{HC} \parallel Sign_{PR} \parallel C_{PR} \parallel T_{ce8})$

Further, HD checks $S_5{}' equals\, S_5$,if not equal HD terminates the session, if equals HD authenticate the $C_e$and computes key $K_5 = h(F_{PID} \parallel U_{HID} \parallel MID)$, and decrypts $(p_{rh}, p_{rb}) = D_{K_5}(C_{PR})$ and HD checks $V_{PU_{HC}}(Sign_{HC}) = \text{h}(p_{rh)}$and $V_{PU_{PR}}(Sign_{PR}) = \text{h}(p_{rb)}$holds or not. If holds HD takes $p_{rd} = (F_{PID}, D_P)$,encrypts $C_{HD} = E_{K_5}(p_{rh}, p_{rb,}p_{rd})$, then HD produce digital signature $Sign_{HD} = S_{PRD}(h(p_{rd}))$, $S_6 = h(F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{HD} \parallel Sign_{PR} \parallel T_{D3})$, and $SK_{HD} = h(S_6 \parallel F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{HD} \parallel Sign_{PR} \parallel rbg \parallel T_{D3})$. Moreover, HD encrypts $E_6 = E_Z(S_6, Sign_{HD}, C_{HD}, T_{P3})$ and sends message $M_{c4} = \langle E_6, T_{D3}\rangle$ to C_e via insecure communication channel.

3 Upon receiving HD request C_e verifies time stamp between hospital and cloud $T_{ce9} - T_{D3} \leq \Delta T$, if it is does, decrypts message $(S_6, Sign_{HD}, C_{HD}, T_{P3}) = D_{sq_i}(E_6)$, and computes then compute hash value $S_6{}' = h(F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{HD} \parallel Sign_{PR} \parallel T_{D3})$,verifies $S_6{}' equals\, S_6$, if equals C_e authenticate HD and $SK_{CD} = h(S_6{}' \parallel F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{HD} \parallel Sign_{PR} \parallel rbg \parallel T_{D3})$ stores HD record $C_{HD}, Sign_{HD}$. If not equal, it terminate.

3.4. Patient Checkup Phase (PCP)

In this phase, P_R and C_e mutually authenticated, and C_e provides report to P_R. The details as follows:

1. P_R sends F_{PID} , MID, s_{qi} and generates random number $f \in Z_q{}^*$,send message $M_{P4} = \langle F_{PID}\ , MID, s_{qi}, f\rangle$ to C_e via secured communication channel.

2. Upon receiving P_R request C_e verifies time stamp between hospital and cloud $T_{ce10} - T_{P4} \leq \Delta T$,if it is ok, generates random number $a \in Z_q{}^*$,then computes $S_7 = h(SK_{ce} \parallel F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{PR} \parallel \text{fag} \parallel T_{ce11})$, encrypts$E_7 = E_{SK_{CP}}(S_7, HD_{ID}, Sign_{HD}, C_{HD}, a, T_{ce11})$ and send message $M_{c5} = \langle E_7, T_{ce11}\rangle$ to P_R via insecure communication channel.

3. Upon receiving cloud request P_R verifies time stamp between hospital and cloud $T_{P5} - T_{ce11} \leq \Delta T$, if not satisfies, P_R terminates the session. If satisfies, P_R decrypts $S_7, HD_{ID}, Sign_{HD}, C_{HD}, a, T_{ce11})$ =$E_{SK_{CP}}(E_7)$ and computes $S_7{}' = h(SK_{ce} \parallel F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{PR} \parallel \text{ fag} \parallel T_{ce11})$, Further, P_R checks $S_7{}' equals\, S_7$,if not equal P_R terminates the session, if equals P_R authenticate the $C_e$and computes key decrypts $(p_{rh}, p_{rb}, p_{rd}) = D_{K_4}(C_{HD})$ and P_R checks $V_{PU_{HD}}(Sign_{HD}) = \text{h}(p_{rd)}$and $V_{PU_{PR}}(Sign_{PR}) = \text{h}(p_{rb)}$holds or not. If holds P_R encrypts $C_E = E_{K_5}(p_{rh}, p_{rb,}p_{rd})$, then P_R computes $S_8 = h(SK_{ce} \parallel S_7{}' \parallel C_E \parallel Sign_{HD} \parallel Sign_{PR} \parallel T_{D6})$, and encrypts $E_8 = E_{SK_{PC}}(S_8, C_E, T_{P6})$ and sends message $M_{P5} = \langle E_8, T_{P6}\rangle$ to C_e via insecure communication channel.

4. Upon receiving P_R request C_e verifies time stamp between hospital and cloud $T_{ce12} - T_{P6} \leq \Delta T$, if it is does, decrypts message $(S_8, C_E, T_{P6}) = E_{SK_{PC}}(E_8)$, and computes then compute hash value $S_8{}' = S_8 = h(SK_{ce} \parallel S_7{}' \parallel C_E \parallel Sign_{HD} \parallel Sign_{PR} \parallel T_{D6})$, verifies $S_8{}' equals\, S_8$, if equals C_e authenticate P_R and store C_E in database.

4. Security Analysis

4.1. Patient Anonymity (SR1)

In the proposed scheme, the patient facial ID F_{PID} encrypted with hospital center$E_2 = E_{SK_{HC}}(F_{PID}, MID, C_{HC}, S_2, Sign_{HC}, T_{ce3})$using hospital session key $SK_{hc} = h(U_{HID} \parallel S_1{}' \parallel hkg \parallel T_{ce1})$. This can be decrypted only with cloud environment as described in hospital center data upload phase. Moreover, the patient facial ID as image based, so cipher image is unable to reproduce without using proper session keys and decryption process. Therefore, the proposed scheme can fully realize user anonymity.

4.2. Session Key Agreement (SR2)

According to the proposed scheme, the P_R , H_c , and C_e computes session key in each phase. In patient data load phase session key between P_R and $C_e$as follows: $SK_{PR} = h(F_{PID} \parallel U_{HID} \parallel C_{HC} \parallel S_3{}' \parallel lng \parallel T_{ce5})$, $SK_{ce} = h(F_{PID} \parallel U_{HID} \parallel C_{HC} \parallel S_3 \parallel T_{ce5})$, Hospital center data load phase session key between H_C and $C_e$as follows: $SK_{hc} = h(U_{HID} \parallel S_1' \parallel hkg \parallel T_{ce1})$, $SK_{ceh} = h(U_{HID} \parallel S_1 \parallel hkg \parallel T_{ce1})$, In Patient Treatment phase session key between P_R and $C_e$as follows: $SK_{HD} = h(S_6 \parallel F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{HD} \parallel Sign_{PR} \parallel rbg \parallel T_{D3})$ and $SK_{CD} = h(S_6' \parallel F_{PID} \parallel HD_{ID} \parallel C_{HD} \parallel Sign_{HD} \parallel Sign_{PR} \parallel rbg \parallel T_{D3})$. As described, SK generated by three random numbers , one way hash function of each user unique ID's and their combination of digital signatures. So, due to one way hash function property it is tedious to intercept the message from previously captured by adversary.

4.3. Mutual authentication (SR3)

Mutual authentication process is required to ensure only the legal members are communicating each other. In Hospital center data load phase, H_c receives $M_{C1} = \langle E_1, T_{ce2}\rangle$ and check the authentication between hospital and cloud by checking timestamp $T_{hc2} - T_{ce2} \le \Delta T$, and also checks the hash values $S_1' equals\ S_1$. C_e receives $M_{H2} = \langle E_2, T_{hc3}\rangle$ and verifies time stamp between hospital and cloud $T_{ce3} - T_{hc3} \le \Delta T$ and hash values $S_2' equals\ S_2$. In PDLP P_R verifies time stamp between hospital and cloud $T_{P2} - T_{ce5} \le \Delta T$, checks $S_3' equals\ S_3$ and also $p_{rh}{}^*$=p_{rh}. C_e receives $M_{P2} = \langle E_4, T_{P3}\rangle$, then, it verifies time stamp between hospital and cloud $T_{ce6} - T_{P3} \le \Delta T$, verifies $S_4' equals\ S_4$.If any intruder alters the message, it will be recognized by both the legal members during these verifications. In PTP phase, HD message $M_{c3} = \langle E_5, J, T_{ce8}\rangle$ receives and verifies time stamp between hospital and cloud $T_{D2} - T_{ce8} \le \Delta T$, checks $S_5' equals\ S_5$ and also verifies $V_{PU_{HC}}(Sign_{HC}) = \mathrm{h}(p_{rh)}$and $V_{PU_{PR}}(Sign_{PR}) = \mathrm{h}(p_{rb)}$. C_e receives $M_{c4} = \langle E_6, T_{D3}\rangle$verifies time stamp between hospital and cloud $T_{ce9} - T_{D3} \le \Delta T$, checks $S_6' equals\ S_6$.In PCP, P_R receives $M_{c5} = \langle E_7, T_{ce11}\rangle$,verifies time stamp between hospital and cloud $T_{P5} - T_{ce11} \le \Delta T$,and verifies $S_7' equals\ S_7$.Then C_e receives $M_{P5} = \langle E_8, T_{P6}\rangle$time stamp between hospital and cloud $T_{ce12} - T_{P6} \le \Delta T$ and also verifies $S_8' equals\ S_8$. If any differences observed messages will be terminated.

4.4. Impersonation Attack (SR4)

In HCDLP, any E masquerade C_e and eavesdrop the information, $M_{C1} = \langle E_1, T_{ce2}\rangle$ and tries to compute $K_1' = h(U_{HID} \parallel h \parallel T_{hc1})$,$S_1' = h(U_{HID} \parallel h \parallel k \parallel T_{hc1})$. E cannot compute the values due to one way hash properties of U_{HID}, h, k, T_{hc1}. Guessing these specified values are impossible. Furthermore, cannot compute $S_2 = h(SK_{hc} \parallel C_{HC} \parallel Sign_{HC} \parallel T_{hc3})$. It is impossible to impersonate C_e. Assume that E tries to impersonate H_c, breaks the time stamps $T_{hc2} - T_{ce2} \le \Delta T$ and guessed the identity of H_c, $U_{HIE} = U_{HID}$ and random number h, computes $S_1' = h(U_{HIE} \parallel h \parallel k \parallel T_{hc1})$ is not possible due to hash values of $S_1' = h(U_{HID} \parallel h \parallel k \parallel T_{hc1})$.So E cannot impersonate C_e. Similarly in all other phases impersonation attach is not possible.

4.5. Resistance to Replay Attack (SR5)

A replay attack resistance is ensured in each phase by verification of time stamp intervals between the both sender and receiver. Every single phase of proposed scheme produces random number. These are acting as countermeasure for replay attacks. Moreover, it is hard to compute random numbers. So proposed schemes withstand the replay attacks.

4.6. Forward Secrecy (SR6)

Forward secrecy means that when the private secret key of the $H_c, P_{R,} C_e$ is compromised, the secrecy of previously established session keys should not be affected. According to the proposed scheme, in each phase session keys are computed independently so, it is different in each session. Therefore, the proposed scheme can ensure forward secrecy.

4.7. Resistance to Insider Attack (SR7)

In the patient data upload phase, the patient sends $M_{P1} = \langle F_{PID}, MID, T_{P1}\rangle$to C_e , Upon receiving hospital request C_e verifies time stamp if it is ok, then generates random number $l \in Z_q{}^*$,computes $S_3 = h(MID \parallel F_{PID} \parallel C_{HC} \parallel Sign_{HC} \parallel l \parallel T_{ce5})$, encrypts$E_3 = E_{sq_i}(Sign_{HC}, C_{HC}, S_3, U_{HID}, l, T_{ce5})$ and send message $M_{C2} = \langle E_3, T_{ce5}\rangle$to P_R via insecure communication channel. Here the random number l protect face ID from insider attacks. Moreover, it is difficult for an attacker to retrieve the P_R , since the hash function is the one-way function. As such, the proposed scheme can resist insider attacks. Similarly, insider attacks not possible in HCDP, PTP and PCP phases. Hence, the protocol is secured against the insider attacks.

4.8. Patinet Unlinkability (SR8)

In PTP phase, outsider E unable to retrieve patient medical history between patient and doctor by any means of communication channel, because, $Sign_{PR}$ and C_{PR} are available only via secure communication channel during patient data upload phase. So, it is impossible for E to use $Sign_{PR}$ and C_{PR} in PTP. So, this proposed scheme achieved patient unlinkability.

4.9. Doctor Unlinkability (SR9)

According to the proposed scheme doctor had unlinkability because, $Sign_{HD}$ and C_{HD} are available only via secure communication channel during patient data upload phase. So, outsider E unable to retrieve the doctor details.

4.10. Man in the Middle Attack (SR10)

All phases in the proposed scheme must matches the timestamps and session keys to proceed to further steps of every

Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

single phase. If every phase of this proposed scheme, any adversary E successfully enters after matching the timestamps, further E unable to proceed to next step of the phases due to unbreakable collision free one-way hash function session keys. So, man in middle attack is not possible in this proposed scheme.

4.11. Known and Plain Text Attack (SR11)

In this attack, assume that adversary access one or more pain image and its corresponding encrypted image. In our proposed method face id PDL phase, upon receiving patient face id, C_e verifies time stamp using random number computes $S_3 = h(MID \parallel F_{PID} \parallel C_{HC} \parallel Sign_{HC} \parallel l \parallel T_{ce5})$, encrypts$E_3 = E_{sq_i}(Sign_{HC}, C_{HC}, S_3, U_{HID}, l, T_{ce5})$ and send message $M_{C2} = \langle E_3, T_{ce5} \rangle$to P_R via insecure communication channel. Since algorithm produces different and unique encrypted face id with each session of encryption due to random number. Similarly, HDLP, PTP, PCP phases also random number generated to process the further steps of the phases. So proposed method withstands with know and plain text attack.

4.12. Chosen Plain Text Attack (SR12)

Suppose the adversary use the certain plain text image and use the respective encrypted image to extract the secret key. But, in every phase of the proposed algorithm the secret key is encrypted with one way hash function and its digital signature of every user, moreover unique session key is generated to ensure the authentication of the users, so chosen plain text attack is impossible in this proposed algorithm.

5. Performance Analysis

The performance analysis of the proposed scheme is compared with the schemes [1; 2; 3; 4; 5] in this section. Table 3 and 4 shows the results of this comparison.

We use the investigated results of [4] for the purpose of evaluating the computational cost. Table 2 illustrates the time calculation in sec to measure the performance analysis:

Table 2:Time Calculation for Operations

Time Notation	**Description**	**Calculation in sec**
T_{sign}	Verification /execution of signature.	≈0.332
T_A	Asymmetric Encryption/Decryption	≈0.306
T_S	Symmetric encryption / decryption	≈0.009
T_M	Multiplication	≈0.050
T_P	Bilinear pairing	≈0.062
T_H	SHA-1 hash function	≈0.0005

Light weight operations such as ||, ⊗ and ⊕ have been ignored.

Table 3 illustrates that our proposed scheme achieved all security requirements which are predefined compared to different schemes.

Table 4 shows that the computation costs comparison of the schemes. The computation cost for proposed scheme is ≈2.5495 with facial id. As observed that our scheme is produces same computation cost as V. Kumar et al.[4] along with facial ID. However, our scheme has a higher complexity in comparison to V. Sureshkumar et al [2], Mohit et al.[3] and Priyansi et al. schemes. Our proposed scheme is able to meet all the evaluation criteria as facial id is considered.

The following Fig 2 shown the implementation facial ID. The patients sample face ID has taken as the input image[24], encrypted and decrypted through ECC algorithm. As observed from Fig.2, it is clearly illustrated that proposed scheme supports the authentication through facial ID images and it provides more security for the patient's data in the cloud assisted TMIS applications.

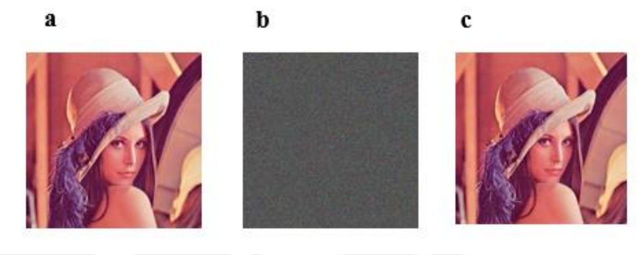

Fig. 2 Facial ID Implementation. (a) Original Face ID (b) Encrypted Face ID, and (c) Decrypted Face ID

The following Table 3 specifies that 'A' is Achieved and 'NA' is not achieved.

Table 3: Security Analysis

Criteria	**Chun-Ta Li.et.al. [1]**	**V. Sureshkumar et al.[2]**	**Mohit .P.et al.[3]**	**V.Kumar et al.[4]**	**Priyansi et al. [5]**	**Ours**
SR-1	NA	A	NA	A	NA	A
SR-2	NA	A	A	A	NA	A
SR-3	A	A	A	A	NA	A
SR-4	NA	A	NA	A	NA	A
SR-5	A	A	A	A	NA	A
SR-6	NA	NA	NA	NA	NA	A
SR-7	NA	A	NA	A	NA	A
SR-8	NA	NA	NA	A	NA	A
SR-9	NA	NA	NA	A	NA	A
SR-10	A	A	A	A	NA	A
SR-11	NA	NA	NA	NA	A	A
SR-12	NA	NA	NA	NA	A	A

Table 4: Comparison of Computational Cost

Schemes	Computation Cost				
	HDUP	PDUP	PTP	PCP	Total computation cost
Chun-Ta Li.et.al.[1]	$11T_{Hash} + 1T_{sign}+3T_S$	$10T_{Hash} + 2T_{sign}+4T_S$	$10T_{Hash} + 3T_{sign}+6T_S$	$8T_{Hash} + 1T_{sign}+2T_S$	$39T_{Hash} + 7T_{sign}+15T_S \approx 2.4785$
V. Sureshkumar et al [2]	$9T_{Hash} + 1T_{Bio}+3T_S$ $4T_{cm}$	$9T_{Hash} + 1T_{Bio}+3T_S$ $4T_{cm}$	$9T_{Hash} + 1T_{Bio}+3T_S$ $4T_{cm}$	$9T_{Hash} + 1T_{Bio}+3T_S$ $4T_{cm}$	$36T_{Hash} + 16T_{cm}+ 12T_S + 4T_{bio} \approx 0.818$
Mohit.P.et al.[3]	$11T_{Hash} + 1T_{sign}+3T_S$	$9T_{Hash} + 2T_{sign}+2T_S$	$9T_{Hash} + 2T_{sign}+2T_S$	$5T_{Hash} + 1T_{sign}+3T_S$	$35T_{Hash} + 6T_{sign}+9T_S \approx 2.248$
V.Kumar et al.[4]	$10T_{Hash} + 1T_{sign}+5T_S$	$11T_{Hash} + 2T_{sign}+ 6T_S$	$11T_{Hash} + 3T_{sign}+6 T_S$	$5T_{Hash} + 1T_{sign}+ 6T_S$	$37T_{Hash} + 7T_{sign}+ 23T_S \approx 2.5495$
Priyansi et al. [5]	$2T_{cm}$	$2T_{cm}$	$2T_{cm}$	$2T_{cm}$	$8T_{cm} \approx 0.4$
Proposed Scheme	$10T_{Hash} + 1T_{sign}+5T_S$	$11T_{Hash} + 2T_{sign}+ 6T_S$	$11T_{Hash} + 3T_{sign}+ 6T_S$	$5T_{Hash} + 1T_{sign}+ 6T_S$	$37T_{Hash} + 7T_{sign}+ 23T_S \approx 2.5495$

6. Conclusion

In this paper, we design and analysed of an image or facial id based mutual authentication scheme using ECC for cloud assisted TMIS. The proposed scheme enhanced mutual authentication via facial id, preserves patient anonymity and withstands the known and chosen plaintext attack for cloud assisted TMIS environment. The performance and security analysis shown that the proposed scheme has better efficiency and security and thus is more desirable for practical applications.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] Chun-Ta Li, Dong-Her Shih, Chun-Cheng Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems", Journal of Computer Methods and Programs in Biomedicine , vol. 157, pp. 191-203,2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] V. Sureshkumar, R.Amin, M.S. Obaidat, I.Karthikeyan, "An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map", Journal of Information Security and Applications, vol. 53, pp. 102539, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohit, P., Amin, R., Karati, A., Biswas, G.P., Khan, M.K., "A Standard Mutual Authentication Protocol for Cloud Computing Based Health Care System", Journal of Medical Systems , vol. 41, no. 4, pp.1-13. April 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Vinod Kumar, Musheer Ahmad, Adesh Kumari, "A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS", Journal of Telematics and Informatics,vol.38, pp.100-117,2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Priyansi P. Chittaranan P., Xiao-Zhi G., Diptendu S.R and Rabindra K.B, "Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps", IEEE Access, vol. 9, pp. 76191-76204, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Chaudhry SA, Khan MT, Khan MK, Shon T. A Multiserver Biometric Authentication Scheme for TMIS using Elliptic Curve Cryptography". Journal of Medical System. vol.40.,no. 11.,pp.230. PMID: 27646969. 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] Amin R, Biswas GP. "An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS", Journal of Medical System 2015 Aug; vol.39,no.8.pp.79. PMID: 26123833. 2015 . [CrossRef] [Google Scholar] [Publisher Link]

[8] Kumar V, Jangirala S, Ahmad M. "An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing Journal of Medical System 2018 Jun 28; vol.42, no.8.,pg.142. PMID: 29956007. [CrossRef] [Google Scholar] [Publisher Link]

[9] Chandrakar, P., Sinha, S. & Ali, R. "Cloud-based authenticated protocol for healthcare monitoring system". Journal of Ambient Intelligence Human Computing , vol.11, pg.3431–3447 (2020).[CrossRef] [Google Scholar] [Publisher Link]

[10] Habek, Muhammed & Genç, Yasin & Aytaş Korkmaz, Nilay & Akkoç, Ahmet & Afacan, Erkan & Yazgan, Erdem. "Digital Image Encryption Using Elliptic Curve Cryptography: A Review". Proceedings of 4th Int. Congress. on Human-Computer Interaction, Optimization and Robotic Applications ,9800074. [CrossRef] [Google Scholar] [Publisher Link]

[11] Rehman S, Talat Bajwa N, Shah MA, Aseeri AO, Anjum A. "Hybrid AES-ECC Model for the Security of Data over Cloud Storage". Electronics. vol.10., no. 21,pp:2673, 2021.[CrossRef] [Google Scholar] [Publisher Link]

Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

[12] Leslie Lamport. "Password authentication with insecure communication", Communications of the ACM, vol.24, no. 11:770772, 1981. [CrossRef] [Google Scholar] [Publisher Link]

[13] Bae-Ling Chen, Wen-Chung Kuo, and Lih-Chyau Wuu. "Robust smartcard-based remote user password authentication scheme", International Journal of Communication Systems, vol.27, no. 2, pp:377389, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[14] Saru Kumari and Muhammad Khurram Khan. "Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme", International Journal of Communication Systems, vol.27, no.12,pp:3939-3955, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[15] Xiong Li, Jianwei Niu, Muhammad Khurram Khan, and Junguo Liao. "An enhanced smart card based remote user password authentication scheme". Journal of Network and Computer Applications, vol.36.,no.5,pp.1365 1371, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[16] An Young-Hwa. "Security improvements of dynamic id-based remote user authentication scheme with session key agreement", IEEE Proceedings of 15th International Conference on Advanced Communication Technology (ICACT), pp.10721076., 2013. [CrossRef] [Google Scholar] [Publisher Link]

[17] Min-Shiang Hwang and Li-Hua Li. "A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no.1,pp.2830, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ding Wang, Debiao He, Ping Wang, and Chao-Hsien Chu. "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing, vol. 12, no.4,pp.428442, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[19] Jing Xu, Wen-Tao Zhu, and Deng-Guo Feng. "An improved smartcard-based password authentication scheme with provable security". Computer Standards & Interfaces, vol. 31, no.4, pp.723728, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[20] Xiong Li, Jieyao Peng, Saru Kumari, Fan Wu, Marimuthu Karuppiah, and Kim-Kwang Raymond Choo. "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity", Journal of Computers and Electrical Engineering, vol.61, pp.238-249, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ya-Fen Chang, Wei-Liang Tai, and Hung-Chin Chang. "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update". International Journal of Communication Systems, vol.27, no.11,pp.3430-3440, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[22] Qi Jiang, Jianfeng Ma, Guangsong Li, and Xinghua Li. "Improvement of robust smart-card-based password authentication scheme". International Journal of Communication Systems, vol. 28., no.2, pp.383393, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[23] Yanrong Lu, Lixiang Li, Haipeng Peng, and Yixian Yang. Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment. Security and Communication Networks, vol. 9, no.11.pp.1331-1339, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[24] Lena Image. Accessed 2023 [Online]. Available: https://en.wikipedia.org/wiki/Lenna