Secure Channel for Financial Transactions in Cloud Environment Using Blockchain Technology

Prabakaran D (dprabakaranmtech@gmail.com)
IFET College of Engineering https://orcid.org/0000-0003-0808-0597
Shyamala Ramachandran
Anna University Chennai University College of Engineering Tindivanam

Research Article

Keywords: Blockchain technology, cloud computing, Elliptical Curve Cryptography, Chaotic Map Confusion and Diffusion algorithm, Security

Posted Date: June 9th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1639189/v1

SECURE CHANNEL FOR FINANCIAL TRANSACTIONS IN CLOUD ENVIRONMENT USING BLOCKCHAIN TECHNOLOGY

Prabakaran.D[1]; Shyamala Ramachandran[2]
[1]Associate Professor, IFET College of Engineering, Villupuram, Tamilnadu, India-605108
dprabakaranmtech@gmail.com
Orcid Id: 0000-0003-0808-0597
[2]Assistant Professor, University College of Engineering- Tindivanam, Tamilnadu, India – 604001
vasuchaaru@gmail.com
Orcid Id: 0000-0001-9635-3131

Abstract— The progression of digital technology impacts the users to migrate from traditional financial transactions to the online transaction system for performing their financial transactions. The existence of cloud computing and its major benefit of access from anywhere promotes financial transactions. The cloud infrastructure supporting performing financial transactions deals with the huge volume of data and it is quintessential to sustain a high level of security to those sensitive credentials in the cloud storage. The conventional cryptographic algorithms hold good in providing a better level of security to the sensitive data in cloud computing but still fall back to advanced attacks against the cloud data storage. Furthermore, the employment of conventional encryption algorithms in securing the cloud data consumes huge execution time, as it has to perform the authentication check for all types of user access including legitimate and non-legitimate accesses. This research article proposes a novel methodology of incorporating blockchain technology to perform online financial transactions in cloud computing with a high level of security, availability, and reduced execution time. This research work employs Blockchain technology integrated with Elliptical Curve Cryptography (ECC) and Chaotic Map Confusion and Diffusion algorithm to perform secured transactions over a cloud network. The interpretation of the proposed method contributes to better performance in the aforementioned parameters than the existing methodologies. The proposed framework is compared with the conventional method of online transactions using Multi-Factor Authentication (MFA) encompassing the Elliptical Curve Cryptography (ECC). The performance analysis proves that the proposed framework exhibits a high level of security along with reduced computational time, encryption, and decryption cost. The proposed work is interpreted with sample dataset and the computational time is reduced.

Keywords: Blockchain technology, cloud computing, Elliptical Curve Cryptography, Chaotic Map Confusion and Diffusion algorithm, Security.

1. Introduction

Individual entity transactions, particularly those involving money, require numerous processes and intermediate technologies to assist their transactions with a high level of confidentiality. The cloud users [1] tends to access the banking server through the third-party service providers [2], where the security of the transactions remains vulnerable to numerous types of attacks [3] like Man-in-the-Middle attack, Session Hijack, Impersonation attack, Denial of Service (DoS) attack, Impersonation attack, etc. As per the cyber security report released by cybertalk.org, the percentage of cyber attacks on financial sectors rise to 238% in the year 2021 [26], when compared to the cyberattacks reported in the year 2020. Various attacks have been launched through Potentially Unwanted Applications (PUA) [4], which on installation leads to the loss of sensitive data like banking credentials to the hackers. Numerous security measures have been undertaken and introduced by cyber security professionals to strengthen the security of the third-party cloud servers such that a high level of security can be achieved during the execution of online financial transactions. Conventional encryption algorithms [5] along with biometric identities have been introduced in the authentication mechanism before accessing the cloud servers. These practices result in providing a better level of security but lack in executing the authentication mechanism at a reduced execution time. The major concerns partaken by the conventional encryption algorithms are listed in the following subsection.

1.1 Drawbacks in Conventional Encryption algorithms in Cloud Services

The major drawbacks of the existing conventional encryption algorithms in safeguarding the security credentials of the cloud services are as follows:

- The existing cryptographic methodologies store the data in the normal database with poor level of security.
- The execution time consumed by the existing cryptographic algorithms is more, which makes the system act sluggish and also leads to the successful launch of cyber attacks by the hackers.

- The existing methodologies in performing transactions in cloud computing possess elevated encryption and decryption costs which reduces the efficiency of the entire system.
- To overcome the aforementioned drawbacks, the introduction of blockchain methodology in cloud computing will provide a better solution and provides a high level of security at a faster rate of services.

1.2 Blockchain Technology

Blockchain is an unalterable database that is capable of sharing across multiple networks and devices. Blockchain technology [6] is an amalgamated version of cryptography, digital signature along with the hash function and it integrates two basic following concepts. It is simple to calculate a checksum over the given data given. This checksum can be calculated using a special hash function. These routines can be programmed to return a value that has always been the same length, regardless of the input length. The hash value, often known as the message digest, is the name given to this value. Another property of the functions is that they must provide the same output (hash value/message digest) when given the same input. A block typically involves a timestamp along with payload in addition to the hash values. Each block has a digital signature [7], which permits any changes to the data since the signature is detected. When new blocks of data are generated, the hash value of the previous block is included in the newly created block. The cloud service providers can leverage the blockchain securely to store the user's authentication credentials and user data. Whenever a new user data is generated and signed, it is written into the blockchain, which provides confidentiality that the data is secured. The personal records stored in the blockchain are encoded and is stored with a private key to maintain its privacy.

1.3 Beneficence of this Proposed Research work

The following are the benefits achieved by the successful implementation of the proposed research work during the execution of financial transactions in the cloud environment.

- This research work proposes a novel framework using blockchain technology to store the cloud user's sensitive data in a secured manner.
- This research work employs Elliptical Curve Cryptography (ECC) [8] for digital signature, which is used to maintain the confidentiality of the stored data in the cloud server.
- The proposed work incorporates Chaotic Map confusion and diffusion process in treating the biometric features and communicating it over the insecure channel.

- The proposed research work declines the computational complexity that already exists in the present methodology.
- The proposed framework mitigates the encryption and decryption cost along with the increase in the level of security.

1.4 Organization of the Research Manuscript:

The organization of the proposed research manuscript is as follows: A detailed literature study is performed in Section 2 to identify the pitfalls of the existing system and to design the objective of the proposed research work. The architecture of the proposed research work is illustrated in Section 3, followed by the performance analysis and comparison of the proposed work with the existing system in Section 4. The work is concluded with a future scope in Section 5.

2. Recent Research Results

Various researchers have been actively involved in designing novel methodologies and algorithms for securing the authentication process while performing financial transactions in a cloud environment. Some of the highlighted research results are considered and analyzed in this section to frame the objective of this proposed research work.

M.A.Saleem and et al. (2021) proposed a secured client-server authentication system using Random Oracle Model [9]. The author incorporated the authentication password, smart card, and user's biometric identity to withstand the vulnerabilities like Impersonation attacks and Man-in-the-Middle attacks. The author employed Elliptical Curve Cryptography (ECC) to perform encryption of sensitive authentication credentials.

Xin Xie and et al. (2021) had designed a novel secured framework based on the lightweight cryptographic algorithms for the Decentralized Data Aggregation (DDA) system [10]. The author employed the Token Controlled Public Key Encryption (TCPKE) scheme to improve the level of security in the DDA system.

Mariem Bouchaala and et al. (2021) had improved the security and the efficiency of the cloud computing authentication mechanism using a key agreement scheme [11] based on the smart card method. The author employed Elliptical Curve Cryptography (ECC) integrated with the fuzzy-based verifier to exhibit a high level of security.

Shengfeng Xu and et al. (2021) had proposed a Key Encapsulation Mechanism (KEM) by Learning Parity with Noise (LPN) [12] to provide security against the post-quantum attacks. The

post quantum attack is launched in the LPN assumptions with a length of 128-bit security level. The proposed scheme holds 50.78MB of public keys and 62.50MB of private keys with 4.54KB of ciphertext.

Saranya and et al. (2021) had designed a Secure Authentication Protocol (SAP) [13] to perform a trustworthy payment process using mobile device. The proposed methodology employed android based payment process using a refined key distribution cryptosystem. The analysis of the designed methodology exhibits better efficiency in computational costs.

Hao Yan and et al. (2021) had presented an identity-based Provable Data Possession (PDP) model [14] to audit and authenticate the certificate verification process. The proposed PDP scheme of authentication process overcomes the certificate management process by performing the identity-based crypto mechanism. The proposed model is proved to be secure by employing the Diffie Hellman assumption.

Surya Parkavi and et al. (2021) had proposed Failure Aware Resource Scheduling (FARS) [15] to mitigate the downfall of the system and the reduction of the performance merits of cloud computing storage. The proposed method encrypts the data file before storing it in cloud storage and decrypts using One Time Password (OTP) during the retrieval process.

Vishesh P.Gaikwad and et al. (2020) had proposed a Chaotic hash function [16] to achieve user anonymity in Telecare Medicine Information System (TMIS). The proposed model incorporates Random Oracle (RO) model for providing security against cyber attacks. The performance analysis of the proposed model exhibits high security and low computational costs.

Fagen Li and et al. (2018) had designed a heterogeneous user authentication model [17] for establishing secure keys in a client-server environment. The key establishment between the server and the client makes the communication more secured. The proposed model introduces heterogeneous user authentication and key establishment protocol using signcryption scheme. The performance analysis of the proposed scheme exhibits reduced computational costs.

Prabakaran and et al. (2022) had introduced Multi-Factor Authentication (MFA) [18] mechanism using Elliptical Curve Cryptography (ECC) and secured the session key using the individual's voice print feature. The proposed framework exhibits a high level of security against network vulnerabilities.

2.1 Identified Research Gaps

Despite the above research results the following are the major drawbacks that persist which question the security level of the third-party transactions in cloud computing.

- The existing methodologies tend to perform the multi-factor authentication mechanism to all incoming service requesting users including legitimate users, thus leading to the increased period of processing the service requests.
- The existing methodologies incorporated large key values to enhance the rigidity against any sort of attack, leading to increased computational overhead.
- The existing methodologies fail to save the transactions history in the cloud server, as it requires more space and is highly vulnerable to cloud server attacks.
- The process of performing mutual authentication between the user and the third party cloud server increases the integrity of the service, followed by an increase in the time span to serve the incoming service requests.

2.2 Objectives of the Proposed Work

The aforementioned research gaps act as a basement for this proposed research work and the objectives are framed to overcome those drawbacks.

- To design a framework that performs a multi-factor authentication process for the identification of anomalies in the pattern of user service requests.
- The proposed work is composed of a blockchain that interlinks the previous histories of third-party transactions, such that to detect the pattern anomaly in user service requests.
- To diminish the computational time, and the cost incurred for encryption and decryption during the third party transactions.

3. Proposed Work

The proposed method of executing secure third-party financial transactions through cloud computing involves a straightforward approach and needs multi-factor authentication on divagation in the transaction records stowed in the blockchain. The proposed architecture provides an enhanced level of security to third-party transactions with a reduced encryption and decryption cost. This section defines the phases involved in the proposed method of blockchain-based secured third party transactions through cloud computing.

3.1 Preliminaries of Proposed Scheme:

The bilinear mapping technique assists the practice of performing the pairing among the cryptographic groups with the third group as represented in equation 1.

$$e: G_1 \times G_2 \rightarrow G \quad (1)$$

Where G_1, G_2 and G represents the multiplicative cyclic group or prime order "p", which satisfies the bilinearity property as represented below.

1. Bilinear property: The bilinear property states that the h_1, h_2 are the elements of group G and x,y are the elements belongs to Z_p as represented in equation 2.

$$e(h_{x1}, h_{y2}) = e(h_1, h_2) \times x \times y \quad (2)$$

The notations used to describe the proposed methodology are listed in Table 1.

Table 1: Symbols and Representations employed in Proposed Model

Symbol	Description
L_i	Location Index of the User (U_i)
U_i	User
p	Biggest Prime number
G_{g1}	Generator of Group G_1 (Additive group)
G_{g2}	Generator of Group G_2 (Multiplicative group)
e	Bilinear pair
H_{g1}	Hash Value of Group G_1
H_{g2}	Hash Value of Group G_2
U_{ID}	User Identity
β_{Ki}	Public Key of the User
ρ_{Ki}	Private Key of the User
β_{KB}	Public Key of the Banking Server
ρ_{KB}	Private Key of the Banking Server
LPW_i	Low entropy password
C_R	Cipher Text
r_{Ki}	Registration Key
B_{Ui}	Block creation for User (U_i)
AS_i	Authentication Server
D_{ID}	Device Identity

H_{Bui}	Hash value Generated for User (U_i)
$H_{Bui\ (R)}$	Hash value Registered for User (U_i)
R_{KB}	Registration Key
B_{Ui}	Block Generated for User (Ui)
SK_i	Session Key
$T_1 – T_4$	Time Stamp
$N_1 – N_3$	Nonce
E	Encryption
D	Decryption
SFA_{Ui}	Second Factor Authentication of User (Ui)
$CSFA_{Ui}$	Cipher Text of User's Biometric Identity
$PSFA_{Ui}$	Plain Text of User's Biometric Identity
F_{Ui}	Extracted Feature of User Ui
F_{UiR}	Registered Feature of User Ui

The proposed architecture depicted in Figure 1, enhances the trust among the users, third party cloud servers and database servers by resolving the concerns registered in the identity authentication phase.

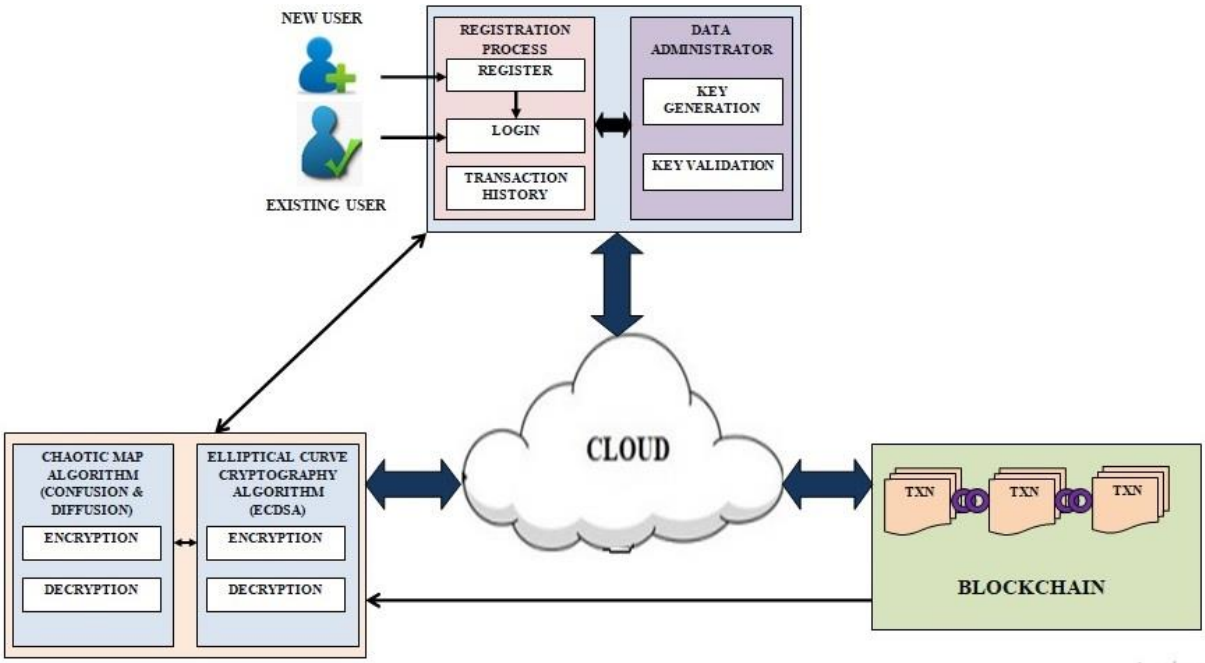

Figure 1: Architecture of the proposed system

This system provides security against identity attacks in cloud computing and delivers sustainable security among the user and the third-party service providers. The proposed architecture is composed of the initialization phase, registration and key generation phase, authentication phase using Elliptical Curve Cryptography (ECC), blockchain phase, and Chaotic map confusion-diffusion phase. The proposed work is intended to secure third-party financial transactions through cloud computing from malicious attacks and unauthorized access attempts. This proposed work employs blockchain technology, such that to provide a high level of robustness against attacks like Man-in-the-Middle attacks, eavesdropping attacks, crypto attacks, Denial of Service (DoS) attacks, Session hijacking attacks, and Password Discovery attacks. The proposed work employs Elliptical Curve Cryptography (ECC) algorithm to perform encryption and decryption of the authentication credentials of the authorized user. The second factor of authentication is scrambled (confusion and diffusion) using a chaotic map algorithm during the authentication verification phase in the cloud server. The copy of the transaction detail is stored in the blockchain as a group of blocks for forthcoming verification and authentication purposes.

3.2 Initialization Phase:

The block initialization phase is comprised of two stages namely, specifying the parameters of the proposed work followed by the generation of pair of keys for the user and the block.

1. The block initialization phase generates the pair of keys using an algorithm like MD5 algorithm and characterizes the parameters of the proposed system. The representation of the initialization phase is defined in terms of key pair and is represented as (L_i, α_1, α_2, p, G_{g1}, e, H_{g1}, H_{g2}).
2. The second process implicates the generation of pair of keys utilizing consensus theorem employing blockchain node.

3.3 Registration and Key Generation Phase:

The Registration and Key generation phase enable a new user to enroll themselves and the user (U_i) generates a unique ID (U_{ID}) along with the generation of the public key (β_{Ki}) and Private key (ρ_{Ki}). The authentication credential elements are shared with the network administrator in an encrypted form using Elliptical Curve Cryptography (ECC). In turn, the network administrator

shares the secure Session Key (S_{Ki}) to accomplish the mutual authentication process. The pseudocode for the registration phase is illustrated in Table 2.

Table 2: Pseudocode for Registration phase for New users

Algorithm 1: *Registration Phase*

1: ***Input***: User Identity (U_{ID}); Public Key (β_{Ki}); Low entropy password (LPW_i)

2: ***Output***: Cipher Text (C_R); Registration Key (r_{Ki}); Block creation (B_{Ui})

3: ***Process***: Registration phase

4: The Authentication Server (AS_i) elects to employ Elliptic Curve by possessing the Banking Server (BS_i) and identifies base points $G_1(x_1, y_1)$; $G_2(x_2, y_2)$; G(x,y); E(a,b)

$$y^2 = x^3 + aX + b \quad (3)$$

5: User (U_i) key pair generation:

$$\beta_{Ki} = \rho_{ki} * G_1 * G_2 \quad (4)$$

where, pK_i is the private key is any largest prime number elected in random.

6: Banking server (BS_i) key pair generation:

$$\beta_{KB} = \rho_{kB} * G_1 * G_2 \quad (5)$$

where, ρ_{KB} is the private key is any largest prime number elected in random.

7: Encryption process: (at User End)

$$LPW^* = h(LPW_i||U_{ID}) \quad (6)$$

$$C_R = E_{\beta K_B}(U_{ID}||LPW_i||LPW^*||\beta_{Ki}||D_{ID,}T_1) \quad (7)$$

8: Decryption Process: (Network Administrator)

$$P_R = D_{\rho K_B}(C_R) \rightarrow U_{ID};\ LPW_i;\ LPW^*; \beta_{Ki}; D_{ID} \quad (8)$$

9: Generation of Hash Value:

$$H_{BU_i} = h(U_{ID}||LPW^*||D_{ID}) \quad (9)$$

10: Issue of Registration Key – Registration Confirmation:

$$R_{KB} = E_{\rho K_B}(U_{ID}||\beta_{Ki}||r_{ki}, T_2) \quad (10)$$

11: Registration confirmation:

$$r_{Ki} \leftarrow D_{\rho K_i}(R_{KB}) \quad (11)$$

12: Block creation:

$$CB_{U_i} \leftarrow E_{\rho K_i}(U_{ID}||\beta_{Ki}||r_{ki}, N_1) \quad (12)$$

$$B_{U_i} \leftarrow D_{\rho K_B}(CB_{U_i}) \quad (13)$$

13: end processes

14: end

3.4 Login (Authentication) Phase:

The login phase or user authentication phase is the gateway of the proposed system which executes authentication inspections for the entire incoming users. The authentication phase involves user id (U_{id}), Device Identity (D_{ID}); Authentication Server with Data Administrator, and Banking Server (BS_i). In this phase, the user tends to succeed in the authentication phase by furnishing the user id (U_{id}) with the Low Entropy password (LPW). The system creates a strong password based on the User's Low entropy password and extracts the Device Identity (D_{id}) to validate the user's authentication. The pseudocode for the blockchain-based authentication phase is illustrated in Table 3.

Table 3: Algorithm for Login (Authentication) Phase

Algorithm 2: *Login (Authentication) Phase*

1: **Input:** User Identity (U_{ID}); Low Entropy Password (LPW)
2: **Output:** Session Key (SK_i)
3: **Process:** Authentication Phase
4: The User provides the User Identity (U_{ID}) along with the Low Entropy Password (LPW)
5: $CA_i = E_{pK_i}(U_{ID}, LPW, D_{ID}||T_3)$ (14)
6: The Network administrator verifies for the matching of the basic authentication credentials.
7: if ($U_{ID} = U_{IDR}$)
8: {
9: if (LPW = LPW_R) // Perform Credential matching
10: else
11: Deny login phase with report, "User ID not Registered"
12: {
13: if ($H_{Bui} = H_{Bui\ (R)}$)
14: {
15: Deny login phase with report, "Password Wrong"
16: Session Key $SK_i = E_{\beta K_B}[h(r_i \| D_{ID} \| U_{ID})||N_2]$ (15)
17: else

18: {

19: Requesting for Second Factor Authentication (SFA_{Ui})

20: $SFA_{Ui}: (CSFA_{Ui}) = E_{CMCD}(F_{Ui}[B_{Ui}], N_3)$ // Chaotic Map confusion and diffusion of Biometric authentication described in Section 3.6

21: $SFA_{Ui}: (PSFA_{Ui}) = D_{CMCD}(F_{Ui}[B_{Ui}], N_3)$

22: if ($F_{Ui} = F_{UR}$)

23: Update Hash value in blockchain as in Section 3.5. and equation 16 and 17

24: Session Key $SK_i = E_{pK_B}[h(r_i \| D_{ID} \| U_{ID}), N_2]$

25: Access Granted

26: else

27: Deny login request

28: end if

29: end if

30: end if

31: end if

32: end

The user U_i on providing proper authentication credentials will be granted with the service. In turn, the observation of different service pattern from the users tends to variation in the hash value leading to the requisition of the Second Factor Authentication (SFA_{Ui}) of the authenticated user.

3.5 Hash Value Generation using Blockchain Technology

Blockchain technology verifies the user's authentication process and the hash value function generated using the transaction between the user and the banking server. The transactions performed by the user are will be stored in the hyper-ledger technology [19] which is a distributed enterprise-grade that provides a high level of security. The chain of blocks is composed of multiple transactions which are composed of transaction id, previous transaction id, user's public key, low entropy password, chain code function, functional parameters, etc as depicted in Figure 2. The chain code of the function in the hyper ledger blockchain technology is composed of the secure container and a registry.

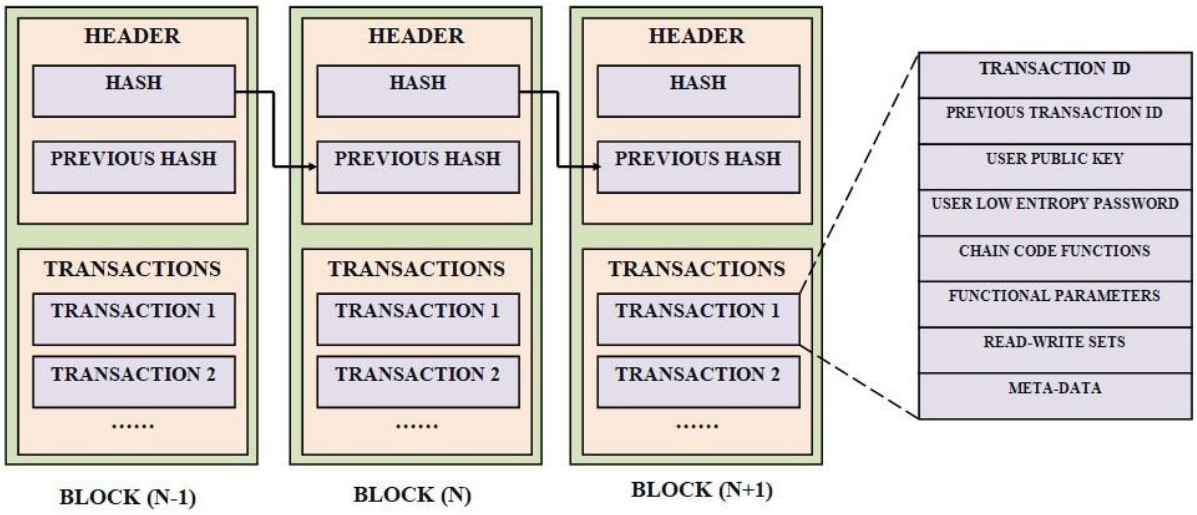

Figure 2: Block creation- Blockchain technology

The Figure 2 depicts the components involved in the generation of hash function for the series of blocks created in the blockchain technology. The blockchain is composed of series of blocks and each block is bounded with hash value, transactions performed between the user (U_i) and the banking server (BS_i), iterations, time stamp and the hash value of the previous block. The generation of hash value is illustrated in equation 16 and 17.

$$HB_{Ui}(n) = F_{HH}(U_{ID}, D_{ID}, S_{ID}, T_{ID}, CC_i, HB_{Ui}(n-1)||T_2, 255) \quad (16)$$

$$HB_{Ui}(n+1) = F_{HH}(U_{ID}, D_{ID}, S_{ID}, T_{ID}, CC_i, HB_{Ui}(n)||T_2, 255) \quad (17)$$

The chain of blocks has been created based on the hash value generated by incorporating Secure Hash Algorithm (SHA-256) as depicted in Figure 3.

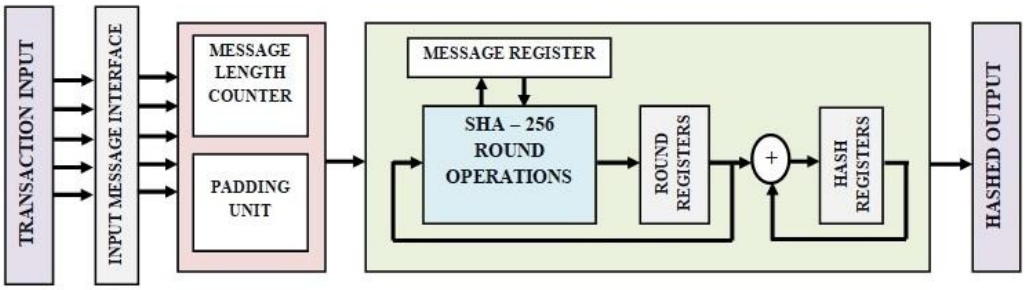

Figure 3: Secure Hash Algorithm (SHA-256)

The incoming message digest from the user U_{ID} is performed with Secure hash Function (SHA-256). The new hash function is generated whenever the comparison of existing hash value is not matched but with matching credentials.

3.6 Confusion and Diffusion using Chaotic Map Algorithm:

The chaotic map algorithm [20] is employed in the proposed system of securing the multifactor authentication process [23]. The deviation in the hash value leads to the second factor authentication, to which the user has to provide the biometric identity. The input biometric identity is treated with chaotic map confusion and diffusion process to misalign the features of the input biometric identity. In turn, the banking server (BS_i) performs the reverse decryption process of Chaotic map diffusion and confusion process to retrieve and to perform second factor authentication verification process. The confusion and diffusion process is depicted in Figure 4. The confusion process involved "m" number rounds and diffusion process with "n" rounds of rotation with chaotic code generated by the chaotic code generator. The secret key for the encryption is the user's private key (ρ_{Ki}) while the secret key for the decryption is the private key of the banking server. After the process of confusion and diffusion, the resulting pattern is again rotated for "x" rounds for further rotation of the input plain biometric feature. The purpose of executing this confusion and diffusion process is to safeguard the biometric features during the transmission in the insecure cloud channel.

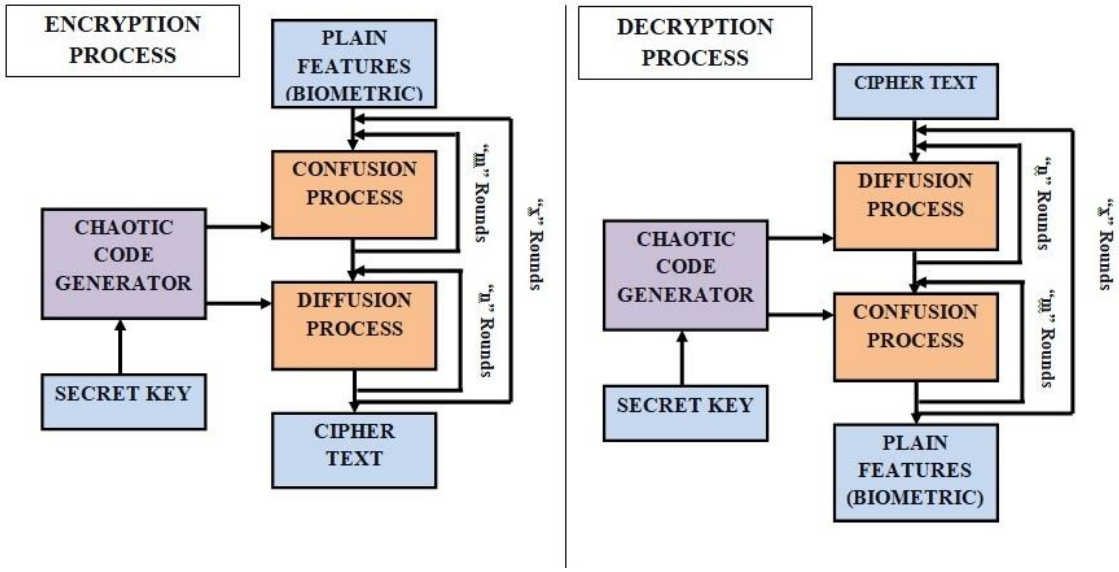

Figure 4: Chaotic Map Confusion and Diffusion Process

The encryption and decryption process is bounded to 256 bits. The decryption process is a reverse process of encryption in which the diffusion process is followed by the confusion process with "n" and "m" number of rotational rounds respectively. The algorithm for the chaotic map encryption and decryption process is illustrated in Table 4 (a) and (b) respectively.

Table 4: (a) Chaotic Map Encryption process; (b) Chaotic Map Decryption process

Algorithm 3: Encryption Process

1: **Input:** Plain Text (Biometric features)
2: **Output:** Cipher Text
3: **Process:** Chaotic Map Confusion and Diffusion (Encryption)
4: procedure Confusion process
5: $F[X,Y]_{i\times j} = Bakersmap(\rho_{Ki}, x_i, y_j)$
6: for i=1 to m; j = 1 to n
7: do
8: $x = X(i)$ and y = Y(j)
9: $C_1 = swap[I(x,y) and\ I(i,j)]$
10: end for
11: Close
12: procedure Diffusion process
13: $F[X,Y]_{i\times j} = Bakersmap(pK_i, x_i', y_j')$
14: for i=1 to n; j = 1 to m
15: do
16: $x = X(i)$ and y = Y(j)
17: $C_2 = mod[X(i-1), Y(j-1), 255]$
18: end for
19: Close
20: procedure Rotation
21: $C(i,j) = mod[(x \oplus C_1 \oplus C_2), 255]$
22: $CSFA_{Ui} \leftarrow C(i,j)$ // Cipher Text
23: end

Algorithm 4: Decryption Process

1: **Input:** Cipher Text
2: **Output:** Plain Text (Biometric features)
3: **Process:** Chaotic Map Confusion and Diffusion (Decryption)
4: procedure Diffusion process
5: $C[X,Y]_{i\times j} = Bakersmap(pK_{Ui}, x_i', y_j')$
6: for i=1 to n; j = 1 to m
7: do
8: $x = X(i)$ and y = Y(j)
9: $P_1 = mod[X(i-1), Y(j-1), 255]$
10: end for
11: Close
12: procedure confusion process
13: $C[X,Y]_{i\times j} = Bakersmap(pK_{Ui}, x_i, y_j)$
14: for i=1 to m; j = 1 to n
15: do
16: $x = X(i)$ and y = Y(j)
17: $P_2 = swap[I(x,y) and\ I(i,j)]$
18: end for
19: close
20: procedure Rotation
21: $P(i,j) = mod[(x \oplus P_1 \oplus P_2), 255]$
22: $PSFA_{Ui} \leftarrow P(i,j)$ // Plain Text
23: end

On successful verification of the second factor authentication, the session key (SK_i) is generated and is sent to the user, followed by the updation of hash value in the blockchain as a new transaction. This framework provides a high level of security during the third party transactions [24] in cloud computing, with reduced transaction duration when compared to the previous works [18].

4. Performance Analysis

The performance analysis of the proposed work is two folded and is analyzed based on level of security and the computational costs. The proposed work is tested against various types of cloud computing attack and the level of rigidity against the attack is verified. Based on the security analysis, the secure factors of the proposed work are highlighted. Varieties of case studies have been performed with multiple attacking factors.

4.1 Theorem 1: Secrecy towards Man-in-the-Middle Attack:

The Man-in-the-Middle Attack is a critical threat to the cloud services, which tends to alter the communication between the user (U_i), Authentication Server (AS_i) and Banking Server (BS_i). The proposed system exhibits high level of rigidity against the Man-in-the-Middle attack as the private key of the user and Banking Server (BS_i) are known only to the self and not disclosed to other parties. The Registration Key (R_{KB}) can be decrypted only by the private key of the User (U_i) and hence the registration process is proved to be secure one. The Hash value $CB_{U_i} \leftarrow E_{\rho K_i}(U_{ID}||\beta_{Ki}||r_{ki}, N_1)$ generated for the user (U_i) can be decrypted by the private key, proving that the framework provides high level of secrecy against the Man-in-the- Middle attack. The messages, $C_R = E_{\rho K_B}(U_{ID}||LPW_i||LPW^*||\beta_{Ki}||D_{ID,}T_1)$; $CB_{U_i} \leftarrow E_{\rho K_i}(U_{ID}||\beta_{Ki}||r_{ki}, N_1)$; $SK_i = E_{\rho K_B}[h(r_i\|D_{ID}\|U_{ID})||N_2]$ are encrypted and decrypted by the private keys and is proved to be highly secured. In case of achieving success in the attacking process, the hash value of the block created for the authenticated user will vary due to deviation in the transaction pattern, leads to the requisition of second factor authentication from the user. The second factor authentication cannot be duplicated as it is the biometric identity and the duplication will leads to the failure of authentication verification process. Thus the proposed work is proved to maintaining high level of secrecy against the Man-in-the-Middle attack.

4.2 Theorem 2: Counter against Password Guessing attack:

The password guessing attack is a type of attack in which the attacker tends to perform brute forcing process to determine the actual Low Entropy Password of the legitimated user. The proposed method of performing secure transmission in cloud computing environment exhibits high level of security against such type of attacks using blockchain technology. The entire framework does not solely rely on the Low Entropy Password but also relies on multiple factors like blockchain technique and Secure Second factor authentication process. The attacker on succeeding in identifying the password

has to pass over the blockchain process in which the hash values are compared with the previous blocks using $H_{Bui} = H_{Bui\ (R)}$. Failing to equal the hash values, leads to the second factor authentication which cannot be guessed as it relies on the biometric of the legitimate user. The hash value of the blockchain is generated using $HB_{Ui}(n) = F_{HH}(U_{ID}, D_{ID}, S_{ID}, T_{ID}, CC_i, HB_{Ui}(n-1)||T_2, 255)$, which involves multiple factors and the probability of identifying all these factors consumes huge time which is more than the time stamp T_2.

4.3 Theorem 3: Counter against Biometric attack:

The non-equaling of the hash value in blockchain technology leads to the second factor authentication, which normally requests for the legitimate user's biometric features. The biometric features [25] may be normally the user's fingerprint or voiceprint from which the features are extracted using the specified algorithms. The feature is communicated to the authentication server for verification purpose which is prune to attack in the insecure network. The biometric feature is treated with Chaotic Map confusion and diffusion process which mash up the location of the features by $C(i,j) = mod[(x \oplus C_1 \oplus C_2), 255]$ such the cipher text C_1 and C_2 are generated by the random secure key generated by the Authentication Server.

4.4 Theorem 4: Anonymity against Denial of Service (DoS) attack:

The Denial of Service (DoS) attack is the passive type of attack tends to attack the cloud server with an objective to make non-availability of service to the legitimate users. The proposed framework employs the role of device identity (D_{ID}) in its encryption process and in creation of blocks in the blockchain technology by using $HB_{Ui}(n) = F_{HH}(U_{ID}, D_{ID}, S_{ID}, T_{ID}, CC_i, HB_{Ui}(n-1)||T_2, 255)$. The transaction hash value is oriented on the device identity and the session key generated $SK_i = E_{\rho K_B}[h(r_i \| D_{ID} \| U_{ID}), T_4]$ using device identity will be performed only once per session. This prevents the system to generate multiple session keys and thus restricting one user shall be provided with one session key at a time thus preventing Denial of Service (DoS) attack.

4.5 System Performance Analysis

The performance of the system shall be analyzed based on the computational time, encryption cost, and decryption cost. The computational time is the time taken by the framework to respond to the increasing service requests from the users.

4.5.1 Computational Time

The increase in computational time leads to the elapse of time stamp leading to expiry of session key and also leads to the breaking of session key such that the attacker tends to identify the pattern of the session key. In this regard, it is efficient that the computational time must be very low. The performance of the proposed work is compared with the method of performing Multifactor authentication (MFA) [18] to perform transaction in cloud computing network, and with Signature based [22] critical mobile transaction methodology. The computational time for increasing number of service requests is depicted in Figure 5.

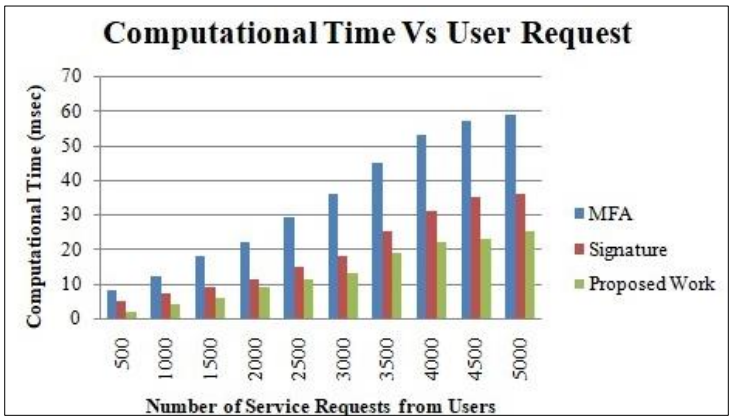

Figure 5: Comparison of Computational Time for Various incoming Service Requests

The Figure 5 depicts the performance of the proposed work with the existing state of art methodologies of employing Multi Factor Authentication (MFA) and Signature based Authentication system. The proposed work is analyzed with sample data set and the computational time is compared with state of art methodologies. The analysis proves that the proposed Blockchain based authentication system consumes reduced computational time of 28msec whereas the MFA exhibits a computational time of 59msec in providing service to the legitimate users. This reduction of computational time is achieved as the second factor authentication is requested to the selective users for whom the hash value is deviated. The legitimate users with non-deviating hash value in the blockchain will be provided with the session key without requesting for second factor authentication.

4.5.2 Encryption Cost

The encryption cost is the time incurred by the proposed framework to perform encryption process. The proposed work employs Elliptical Curve Cryptography (ECC) algorithm to convert the plain text composed of user authentication credentials into cipher text. The Elliptical Curve Cryptography is a secure cryptographic algorithm due to its randomized nature of selecting the key

pair for encryption process. The encryption cost is determined and is compared with the existing method of MFA which employs ECC, Signature based transmission which employs RSA algorithm [21].

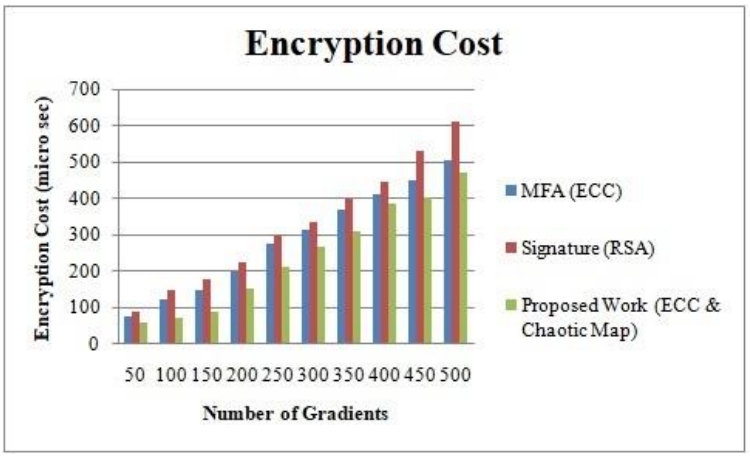

Figure 6: Comparison of Encryption cost among various Cryptographic algorithms

The comparison of encryption cost depicted in Figure 6 proves that the proposed work possess reduced encryption cost when compared to the other works which employs ECC and RSA algorithm for encryption process. The encryption cost for the proposed work is measured to be 479micro seconds while it is observed as 610micro second for signature based encryption process.

4.5.3 Decryption Cost

The decryption cost is similar to the encryption cost, which is the time consumed by the secured proposed framework to perform decryption process. The performance of the proposed work employing ECC and Chaotic map confusion and diffusion process is compared with the works which employs ECC and RSA algorithms for decryption process.

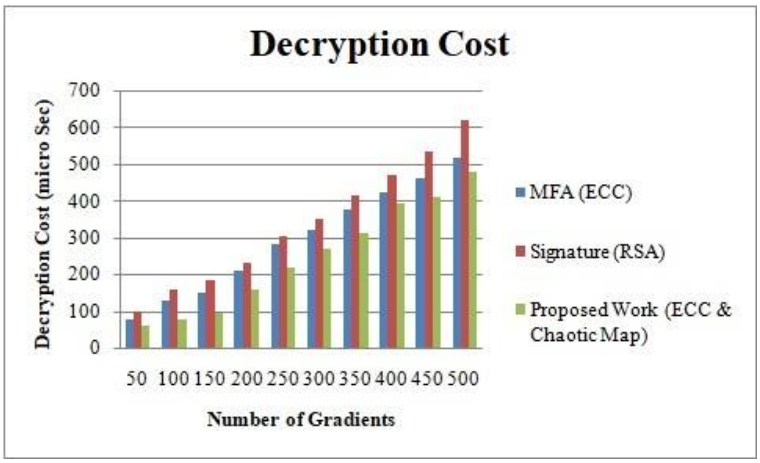

Figure 7: Comparison of Decryption cost among various Cryptographic algorithms

The performance comparison of various decryptions cost with the proposed method employing ECC and Chaotic map confusion and diffusion process is depicted in Figure 7. The analysis proves that the proposed work consumes reduced decryption cost that the existing method of cryptographic algorithms. The decryption cost for the proposed work is measured to be 482micro seconds while it is observed as 630micro second for signature based decryption process.

5. Conclusion

The rapid development of digitization and its enormous applications motivates the involvement of cloud computing in performing financial transactions over insecure network. The cyber attack aiming in gaining ransom had developed worldwide by most nationals and hackers. The attackers tend to launch the cyber attack with an objective to halt the financial transactions and development of a targeted nation or an organization or an individual. This major concern acts as a motivational factor for this research work which employs Elliptical Curve Cryptography and Chaotic Map Confusion and Diffusion algorithm along with the blockchain technology. The employment of blockchain technology in performing secure financial transaction over third party enhances the level of security and provides an efficient transaction process in terms of reduced computation time, encryption and decryption costs. The computation time is reduced by 31.02% and the encryption and decryption costs are reduced by 16% and 11% respectively. The proposed method is tested with various security attacking methods and is proved to be exhibiting high level of resistivity against known attacks of Man-in-the-Middle attack, password guessing attack, Denial of Service attack etc. This framework can be readily implemented in performing financial transactions of banking sectors. This work can be further improved by implementing Artificial Intelligence techniques to differentiate between the transactions of legitimate and illegitimate users in case of deviations in blockchain hash value. This will further mitigate the computational time along with high level of security during the transaction process.

Statements and Declaration

References

[1]. San Murugesan; Irena Bojanova, "Personal Applications of Clouds," in Encyclopedia of Cloud Computing, *IEEE*, 2016, pp.517-523, doi: 10.1002/9781118821930.ch42.

[2]. N. Ghosh, S. K. Ghosh and S. K. Das, "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers," *IEEE Transactions on Cloud Computing*, vol. 3, no. 1, pp. 66-79, 1 Jan.-March 2015, doi: 10.1109/TCC.2014.2328578.

[3]. R. Shyamala and D. Prabakaran, "A survey on security issues and solutions in virtual private network," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 15, pp. 3115–3122, 2018.

[4]. C. Pickard and S. Miladinov, "Rogue software: Protection against potentially unwanted applications," *2012 7th International Conference on Malicious and Unwanted Software*, 2012, pp. 1-8, doi: 10.1109/MALWARE.2012.6461001.

[5]. R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of Cryptography," *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, 2016, pp. 1-4, doi: 10.1109/ICTBIG.2016.7892684.

[6]. Sina Rafati Niya; Eryk Schiller; Burkhard Stiller, "Architectures for Blockchain-IoT Integration1," *Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning , IEEE*, 2021, pp.321-344, doi: 10.1002/9781119675525.ch13.

[7]. A. Sengupta, E. R. Kumar and N. P. Chandra, "Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 398-407, Aug. 2019, doi: 10.1109/TCE.2019.2924049.

[8]. K. Jarvinen and J. Skytta, "On Parallelization of High-Speed Processors for Elliptic Curve Cryptography," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* Vol. 16, no. 9, pp. 1162-1175, Sept. 2008, doi: 10.1109/TVLSI.2008.2000728.

[9]. Muhammad Asad Saleem, SK Hafizul Islam, Shafiq Ahmed, Khalid Mahmood, Majid Hussain, "Provably secure biometric-based client–server secure communication over unreliable networks", *Journal of Information Security and Applications*, Vol. 58, 102769, 2021.

[10]. Xie, Xin & Chen, Yu-Chi. (2021). Decentralized Data Aggregation: A New Secure Framework Based on Lightweight Cryptographic Algorithms", *Wireless Communications and Mobile Computing*. 2021. 1-12. 10.1155/2021/5565663.

[11]. Bouchaala, M., Ghazel, C. & Saidane, L.A. Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card," *Journal of Super computing*, Vol.78, Pp.497–522, 2022. https://doi.org/10.1007/s11227-021-03857-7

[12]. S. Xu and X. Li, "Chosen-Ciphertext Secure Key Encapsulation Mechanism in the Standard Model," *IEEE Access*, vol. 9, pp. 13683-13690, 2021, doi: 10.1109/ACCESS.2021.3051047.

[13]. Saranya, A, Naresh.R, "Efficient Mobile Security for E Health Care Application in Cloud for Secure Payment Using Key Distribution", *Neural Processing Letters*. 10.1007/s11063-021-10482-1.

[14]. H. Yan and W. Gui, "Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving," *IEEE Access*, vol. 9, pp. 45822-45831, 2021, doi: 10.1109/ACCESS.2021.3066497.

[15]. S.Surya Parkavi, S.Varshini and Naresh.R, “An Efficient Improving Cloud Data Storage Security Using Failure Aware Resource Scheduling Algorithm”, *Turkish Journal of Computer and Mathematics Education,* Vol. 12, No. 13, Pp. 237-242, 2021.

[16]. Gaikwad, Vishesh & Tembhurne, Jitendra & Meshram, Chandrashekhar & Lee, Cheng-Chi., “Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function”, *The Journal of Supercomputing*. 2021, 77. 10.1007/s11227-020-03553-y.

[17]. Li, Fagen & Wang, Jiye & Zhou, Yuyang & Jin, Chunhua & Islam, SK, “A heterogeneous user authentication and key establishment for mobile client–server environment”, *Wireless Networks*, 2020. 26. 10.1007/s11276-018-1839-4.

[18]. D. Prabakaran and S. Ramachandran, "Multi-factor authentication for secured financial transactions in cloud environment," *Computers, Materials & Continua*, vol. 70, no.1, pp. 1781–1798, 2022.

[19]. B. Sowmiya, E. Poovammal, K. Ramana, S. Singh and B. Yoon, "Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server," *IEEE Access*, vol. 9, pp. 138245-138253, 2021, doi: 10.1109/ACCESS.2021.3115238.

[20]. C. Fu, Y. -F. Shan, M. -Y. He, Z. -Y. Yu and H. -L. Wu, "A New Medical Image Encryption Algorithm Using Multiple 1-D Chaotic Maps," *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2018, pp. 2055-2060, doi: 10.1109/SMC.2018.00354.

[21]. R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status," *IEEE Access*, vol. 9, pp. 155949-155976, 2021, doi: 10.1109/ACCESS.2021.3129224.

[22]. M. Marian, A. Cusman, F. Stîngă, D. Ionică and D. Popescu, "Experimenting With Digital Signatures Over a DNP3 Protocol in a Multitenant Cloud-Based SCADA Architecture," *IEEE Access*, vol. 8, pp. 156484-156503, 2020, doi: 10.1109/ACCESS.2020.3019112.

[23]. D. Prabakaran and R. Shyamala, “A review on performance of voice feature extraction techniques,” *3rd Int. Conf. on Computing and Communications Technologies, Chennai*, Tamilnadu, India, pp. 221–231, 2019.

[24]. S. K. Hafizul Islam, “Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps,” International Journal of Information Sciences, vol. 312, pp. 104– 130, 2015.

[25]. Prabakaran. D and S. Ramachandran, "Secure Key Generation from Speech signal Using Enhanced MFCC Algorithm," *2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, 2021, pp. 1-5, doi: 10.1109/ICMNWC52512.2021.9688398.

[26]. https://www.cybertalk.org/2021/06/25/special-report-security-for-financial-firms-2021

Statement and Declaration

Funding Statement: The authors declare that no funds, grants or other support were received during the preparation of this manuscript.

Competing Interests: The authors have no relevant financial and non-financial interests to disclose.

Author Contributions: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by **Prabakaran.D**, and **Shyamala Ramachandran.** The first draft of the manuscript was written by **Prabakaran.D** and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Data Availability: Data will be made available on reasonable request.

Authors Bibliography

Prabakaran.D completed his Bachelor of Engineering (B.E.) in Electronics and Communication Engineering and Master of Technology (M.Tech.) in Applied Electronics. He is currently pursuing his research (Ph.D.) in Anna University, Chennai. His area of interest includes, cloud computing and network security. He had published his paper in various leading scopus and SCI indexed journals.

Dr.R.Shyamala had done her Bachelor and Masters degree in Computer Science and Engineering. She completed her Ph.D. in Anna University, Chennai in the Network security domain. Her area of interest covers Network Security, Cloud & Mobile Security and Wireless Sensor Networks. She has published more than 10 research papers in top reputed journals. She is working as Assistant Professor in University College of Engineering Tindivanam, (A Constituent College of Anna University, Chennai).