Computers, Materials & Continua
DOI:10.32604/cmc.2022.019591
Article

Tech Science Press

Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment

D. Prabakaran[1,*] and Shyamala Ramachandran[2]

[1]IFET College of Engineering, Villupuram, 605108, Tamilnadu, India
[2]University College of Engineering-Tindivanam, Tindivanam, 604001, Tamilnadu, India
[*]Corresponding Author: D. Prabakaran. Email: dprabakaranmtech@gmail.com
Received: 19 April 2021; Accepted: 03 June 2021

Abstract: The rise of the digital economy and the comfort of accessing by way of user mobile devices expedite human endeavors in financial transactions over the Virtual Private Network (VPN) backbone. This prominent application of VPN evades the hurdles involved in physical money exchange. The VPN acts as a gateway for the authorized user in accessing the banking server to provide mutual authentication between the user and the server. The security in the cloud authentication server remains vulnerable to the results of threat in JP Morgan Data breach in 2014, Capital One Data Breach in 2019, and many more cloud server attacks over and over again. These attacks necessitate the demand for a strong framework for authentication to secure from any class of threat. This research paper, propose a framework with a base of Elliptical Curve Cryptography (ECC) to perform secure financial transactions through Virtual Private Network (VPN) by implementing strong Multi-Factor Authentication (MFA) using authentication credentials and biometric identity. The research results prove that the proposed model is to be an ideal scheme for real-time implementation. The security analysis reports that the proposed model exhibits high level of security with a minimal response time of 12 s on an average of 1000 users.

Keywords: Cloud computing; elliptical curve cryptography; multi-factor authentication; mel frequency cepstral coefficient; privacy protection; secured framework; secure financial transactions

1 Introduction

Virtual Private Network (VPN) is an emerging technology that turns out to be vital among IT professions, research persons, and the common public in terms of employing the data resources through the cloud server. In this modern digital era, the common public utilizes the cloud resources [1] in the form of online financial transactions and as per the survey by Pew report and American Life project, 51% of users stated that they utilize cloud computing due to its easiness and convenience in accessing the resources. The Virtual Private Network has multiple distinct attributes like elasticity, metered services, broad network access, on-demand self-service, resource pooling, measured service, etc. One noteworthy application of cloud computing is digital

financial transaction using desktop or portable devices like smart phone, laptops, etc. through a cloud server, that drives the economy to scale exponentially. The digital financial transactions [2] are executed by accessing the banking server through a third-party cloud service provider, which provides access by consigning session key on prosperous verification of authentication credentials. The cloud computing in parallel to its notorious advantages also face weak security [3] as it is vulnerable to the attacks [4] introduced by Hackers. Some of the highlighted cyber financial attacks were, RBS World pay Hack (Atlanta, 2008), National City Bank breach (United States, 2010), U.S Federal Reserve bank of Cleveland breach (United States, 2010), Global Payments breach (United States, 2011), Brazilian payments system Attack (Brazil, 2012), JP Morgan Chase Data Breach (United States, 2014), Equifax hack (United States, 2017), City Union Bank SWIFT Attack (India, 2018), Mexican Bank Theft (Mexico, 2018), State Bank of Mauritius (Mauritius, 2018), SBI Breach (India, 2019), Paypal Accounts linked to Google pay abused (United States & Germany, 2020). The hackers target the security credentials by introducing multitudinous means of attacks like Man-in-the-Middle attack, impersonation attack [5], session hijack [6], secure socket layer attack, Denial of Service (DoS) attack [7], eavesdropping [8], password discovery attack and had succeeded in gaining access to the database resources with the authentication credentials earned illegitimately. The Deloitte- India Banking Fraud Survey, edition II, states that 54% of banking attacks were succeeded by hackers in executing the pre-mentioned attacks. Besides, the Quick Heal annual report 2017 mentions that hackers introduce attacks through range of vulnerabilities like Trojan, infectors, worm, Potentially Unwanted Application (PUA), adware, Ransomware. Research has been accelerated in this domain to clear the pit fall of weak security in cloud computing. Despite abundant research and results, the authentication policy [9] prevails weaker and lacks mutual authentication between the user device and cloud authentication servers. The cloud-based authentication server is a multi-cloud server, provide session key to the user on successful affirmation of the authentication process. The hacker manages to gain the session by cracking the authentication verification system. The feeble authentication paves a path to the breach of communication channel security and the integrity of the transmitted data was compromised. The severity of this concern is the motivation for this research work, and its benefaction to resolving this issue is spotlighted as follows.

1.1 Beneficence of the Research Work

(i) This research work proposes a novel framework with Multi-Factor Authentication (MFA) system to strengthen the security using a low entropy password, individual unique biometrics for authentication.

(ii) The influx of Multi-Factor Authentication (MFA) inhibits the hackers from attacking the session by encrypting the credentials and session key by Elliptical Curve Cryptography (ECC).

(iii) This system magnifies the security for third party transactions in the cloud network by preferring voice recognition as an imperative parameter along with customary credentials that include the user name and low entropy password.

(iv) The motive for the preference of voice recognition over different biometrics was these metrics follow image recognition system which can be duplicated whereas the voice recognition has the least possibility of duplication and most recent mobile devices embeds voice sensors for the authentication process.

1.2 Organization of This Research Work

The research paper is organized as follows: Section 2 illustrates the recent research works related to the issues aforementioned in Section 1.1, Section 3 narrates the architecture and the algorithms of the proposed framework followed by the security analysis of the proposed work is done in Section 4. Subsequently in Section 5, the evaluation of proposed system is performed and Section 6 concludes the proposed model.

2 Recent Research Results

Plentiful researchers had introduced several policies to implement a secure authentication process and to thwart hackers from succeeding in their attempt of accessing the cloud resources.

Garg et al. [10] proposed and evaluated a mobile phone-based authentication with a session key agreement approach that provides strong authentication services to SOCKS V5 protocol. This proposed protocol is applicable for mobile devices and employs International Mobile Subscriber Identity (IMSI) number to provide an individual's unique identification. Xie et al. [11] proposed a novel dynamic ID-based anonymous two-factor authenticated key exchange protocol. The proposed model addresses multi-factor authentication and prevents vulnerabilities like a lost-smart-card-attack, offline dictionary attack, lack of forward secrecy. It supports smart card revocation and password update without centralized storage. Soares et al. [12] depicts a system that supersedes the ATM cards and PINs by the physiological biometric fingerprint and iris authentication. The feature of One-Time Password (OTP) affords confidentiality to the users and unfastens the user from reviving PINs. Hafizul Islam et al. [13] recommended a scheme of maintaining a password table in the server which has weak security against server masquerade attack, insider attack and hence backslides to sustain security. Tao et al. [14] proposed an intricate face authentication task on the devices with limited resources; the emphasis is largely on the reliability and applicability of the system. Both theoretical and practical considerations are taken. The final system has achieved an equal error rate of 2% under challenging testing protocols. Preeti et al. [15] presented a strong security protocol of three-factor remote authentication system to provide better security and is much complex in terms of performance and cost. Hafizul Islam [16] designed a protocol that offers computation cost-efficient and robust three-party Password-based Authentication Key Exchange (3-PAKE). The key confirmation is done using extended chaotic maps and smart card. The protocol has proved to be secure in the random oracle model and is certified through simulation of Automated Validation of Internet Security Protocols and Applications (AVISPA) software tic maps and smartcard.

The following are the gaps identified on the existing system through the literature survey are:

(i) Lack of stringent authentication scheme to secure the session key.
(ii) Complex Protocols with high computational cost and is vulnerable to attacks.
(iii) The fragile authentication policies, benefits the attackers masquerade the verification process.

3 Proposed Scheme

3.1 Preliminaries of Proposed Scheme

The practice of pairing among the factors of two cryptographic groups to the third group with a mapping

$$e : G_1 \times G_2 \rightarrow G_T \tag{1}$$

where, G_1, G_2, and G_T are the additive cyclic groups of prime order "q".

The pairing based cryptography satisfies the following properties:

(1) The bilinearity property:

$$\forall x, y \in F_q^*, \forall P \in G_1, \forall Q \in G_2 : e(xP, yQ) = e(P, Q)^{xy} \tag{2}$$

(2) The non-degeneracy policy:

$$e \neq 1 \tag{3}$$

(3) The existence of efficient algorithm for the computation of bilinear pairing function "e".

The notations in the Tab. 1 are used to describe the process throughout the paper.

Table 1: Notations used in proposed model

Symbol	Definition
U_i	User
PS_i	Proxy server
BS_i	Banking server
ECC	Elliptical curve cryptography
PID	Identity of PS_i
BID_i	Identity of BS_i
γ	Proxy server's private key
e_i	Bank server public key
p_i	User's private key selected in random
q_i	User's public key
K_1	Secret key of PS_i for BS_i
K_2	Secret key of PS_i for U_i
K_3	Secret key of BS_i for PS_i
SKAS	Session key between PS_i and AS_i
α	Proxy server public key
PW_i	User low entropy password
$IMSI_i$	Public identity of user U_i
B_i	Nonce
D_i	Random nonce
r_i	Random number chosen by U_i
r_j	Random number chosen by PS_i
V_u	U_i unique voice signal
hw	Hanning window
FFT	Fast fourier transform
dct	Discrete cosine transform
V_i	Session key from V_u
DB_i	PS_i data base
SN_i	Session number of U_i selected by PS_i
SK_i	Session key
IP_i	IP address of BS_i

(Continued)

Table 1: Continued

Symbol	Definition
N1, N2	Nonce
FP_i	Finger print of user
E(.)	Symmetric encryption function (i.e., AES)
D(.)	Symmetric decryption function (i.e., AES)
h(.)	One way hash function
$\oplus$	Bitwise Ex-or operation.
$\|$	String concatenation function
V_a	Acoustic vector of voice sample

The aim to design the proposed model that provides a secure platform for the users in performing secured banking transactions using their mobile devices. The proposed model is composed of components namely mobile device, authentication server, banking server, and the user with valid low entropy password and biometric identity. This system has an elasticity of extending with multiple users and multiple banking servers. This model composed of five phases that take account of registration, user verification, voice coefficient extraction phase using MFCC, session key generation, and shielded transaction phase. Fig. 1 illustrates the system architecture of the proposed model. In this proposed model, the user U_i accesses the BS_i by registering the low entropy password and biometric identity especially the user's voice which is unique. The former has to register themselves to the authentication server using a low entropy password and International Mobile Subscriber Identity (IMSI) number while the later register with the authentication server by generating a key pair.

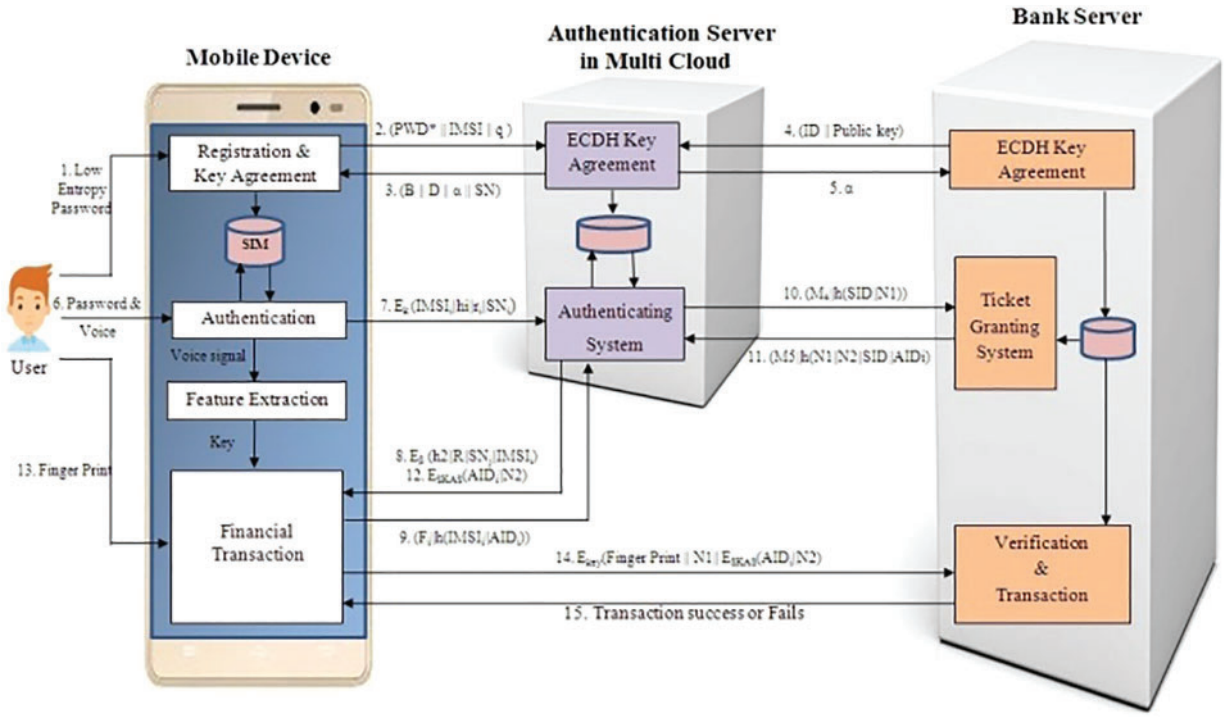

Figure 1: System architecture of proposed model

The user U_i login with password and biometric identity say individual's voice with the authentication server. The authentication server in turn fetches the IMSI of the user device and verifies the digital signature for proper authentication to provide ticket to user the same that received from banking server.

3.2 Algorithm for Registration and Key Agreement Using Elliptical Curve Cryptography

In the Fig. 2, Registration and Key agreement phase were mentioned as registration which involves user's mobile device (U_i), banking server (BS_i) and the authentication server (AS_i). This phase performs two process namely registration and key agreement process where the former is secured as the entire process is performed offline whereas the later uses Elliptical Curve Cryptography (ECC) [17] to generate the session key. The Fig. 2 characterizes the registration process of user U_i and banking server BS_i with the authentication server in multi cloud AS_i.

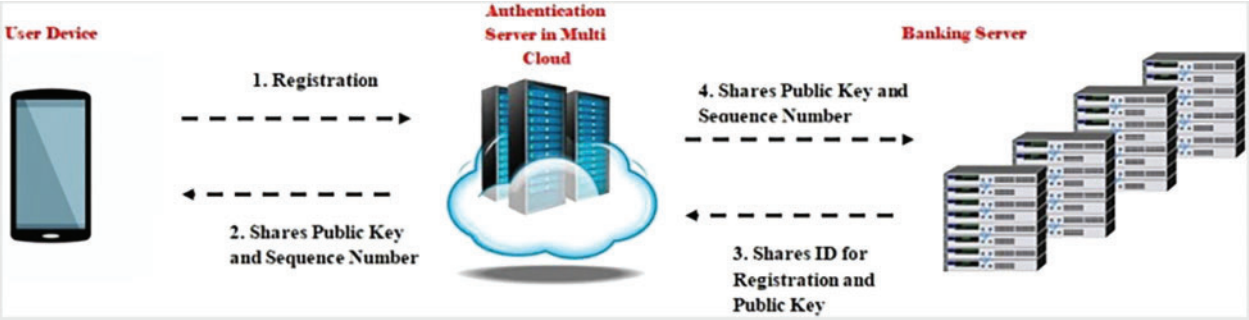

Figure 2: Message flow diagram- registration phase

The algorithm for registration and key agreement is illustrated in Tab. 2.

Table 2: Algorithm for registration and key agreement using elliptical curve cryptography

Algorithm for registration and key agreement using elliptical curve cryptography
1) The AS_i with its identity PID and BS_i choose elliptic curve E, represented by $Y^2 = X^3 + aX + b$ (4) with the base point $G(x_1, y_1)$ and E(a, b).
2) The AS computes public key $\alpha = \gamma * G$, where the private key γ is chosen in random.
3) The BS_i generates $e_i = d_i * G$, where d_i is the BS_i private key.
4) Upon choosing the private key γ, the AS computes and stores secret keys $K_1 = \gamma * e_i$ and $K_2 = \gamma * q_i$, where e_i and q_i are the public keys of BS_i and U_i.
5) The BS_i computes secret key $K_3 = d^i * \alpha$, where α is the public key of AS.
6) The BS_i stores the K_3 and transmits the <BID, e_i> over secure channel.
7) The U_i choose elliptical curve E represented by $Y^2 = X^3 + aX + b$ with the base point $G(x_1, y_1)$ and E(a, b).
8) The AS_i choose private key p_i in random to compute public key $q_i = p_i * G$ and selects its low entropy password (PW_i).

(Continued)

Table 2: Continued

9) The AS_i extracts $IMSI_i$ number for user simcard to compute PW* by performing hash function $PW^* = h(IMSI_i \| PW_i)$ and provides $(IMSI_i, PW_i^*)$ to AS over offline secure channel,
10) On receiving PW*, AS computes $C_i = h(IMSI_i \| \gamma)$ along with the random key B_i by performing $C_i \oplus PW_i^*$ and random nonce $D_i = h(C_i \| B_i)$
11) The AS_i selects a sequence number SN_i (Sets $SN_i = 0$) against U_i and sends $\{\alpha$, Bi, Di, SNi$\}$ to User U_i over a secure offline mode.
12) The U_i computes secret key $K = p_i * \alpha$ and stores $\{K, B_i, D_i, SN_i\}$ in the user mobile device.

The registration and key agreement algorithm is a notarization algorithm involving generation of private key and public key of banking server BS_i and user device U_i. The banking server generates the secret key k_3 and transmits over the secure channel.

3.3 Algorithm for User Verification

This phase involves user U_i, authentication server AS_i and banking server BS_i that performs user authentication and credential verification process to provide a secure session key. In the Fig. 3, the authentication process between the user U_i and the authentication server AS_i is illustrated. In this phase, the U_i provides low entropy password and the individual unique voice to prove its identity authentication process. The voice has been processed by incorporating Mel Frequency Cepstral Coefficient (MFCC) [18] algorithm.

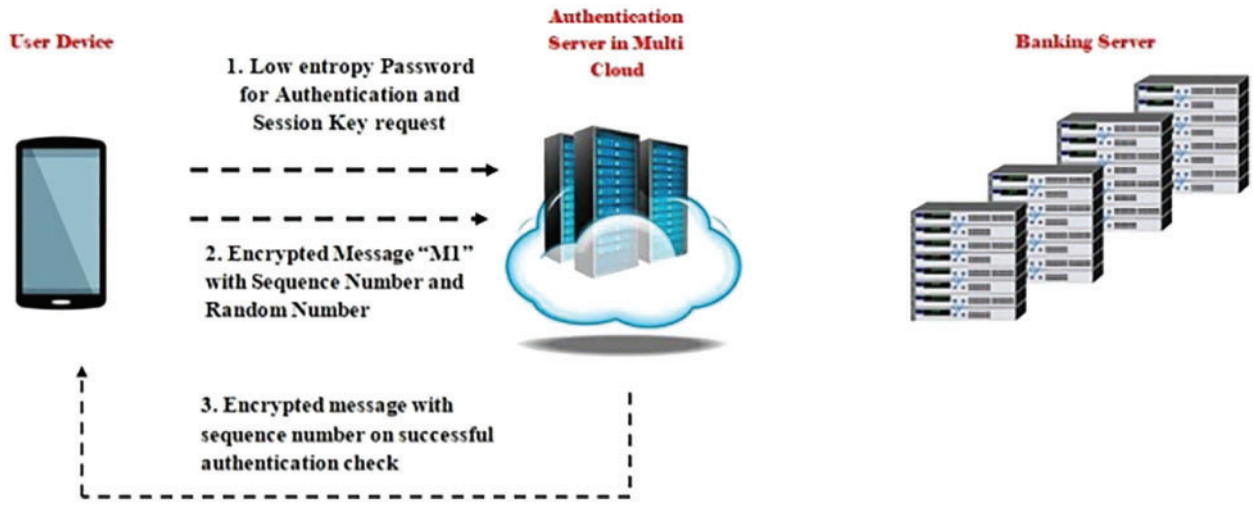

Figure 3: Message flow diagram- user verification phase

The algorithm for user verification is exemplified in Tab. 3.

The user provides its password, which undergoes authentication check and on successful verification, the user device sends login message to authentication server for authentication process for the grant of session key to the user.

Table 3: Algorithm for user verification

Algorithm for user verification
1) The U_i selects r_i and computes $PW'_i = h(IMSI_i \| PW_i)$
2) Utilizing PW'_i, U_i computes $C_i^* = B_i \oplus PW'_i$ and $D_i^* = h(C_i^* \| B_i)$ to compare and check if $D_i^* = D_i$ and to approve the authentication process.
3) The relation $D_i^* \neq D_i$ leads to authentication failure and process termination, whereas the value equality leads to $SN_i = SN_i + 1$ and calculates $h_i = h(C_i^* \| r_1 \| SN_i \| IMSI_i)$.
4) The U_i transfers AS_i an AES encrypted $M_1 = E_K(IMSI_i \| h_i \| r_i \| SN_i)$ over insecure channel.

3.4 Algorithm for Voice Coefficient Extraction Using Mel Frequency Cepstrum Coefficient (MFCC)

The voice V_u of the U_i acts as the major credential and is recorded through the U_i device. The V_u express the U_i gender, emotion and ease the identification process of U_i. Several voice feature extraction algorithms like Linear Predictive Coefficients (LPC), Mel Frequency Cepstral Coefficients (MFCC) and Relative Spectra filtering of log domain coefficients (RASTA) were in practice, among which the Mel Frequency Cepstral Coefficient (MFCC) algorithm provides better accuracy [19], low error rate, high recognition rate, and faster response subject to utilization of self data set. The MFCC provides better V_u coefficients V_i and is well aligned as of human ear's perception that cannot exceed the frequency limit of 1 KHz. The Fig. 4 elucidates the process implicated by MFCC algorithm in extracting the voice coefficients.

Figure 4: Message flow diagram- session key generation phase

The MFCC technique involves pre-emphasis, sampling and windowing process, performing Fast Fourier Transform (FFT), Mel filter bank, performing discrete cosine transform to produce mel coefficients. The MFCC algorithm is executed in MATLAB R2013a version and for the reason that is simpler and creation of better coefficients; the MFCC is implemented in this proposed system to create credentials for authentication process.

The user gratifying the authentication process utilizes session key and providing valid biometric finger print, access BS_i to perform successful transaction. The MFCC accepts the Ui voice input V_i recorded through microphone is continuous in time and is represented as v(t). The algorithm for the voice coefficient extraction using Mel Frequency Cepstrum Coefficient (MFCC) is illustrated in Tab. 4.

Table 4: Algorithm for voice coefficient extraction using Mel frequency cepstrum coefficient

Algorithm for voice coefficient extraction using Mel frequency cepstrum coefficient

1) The v(t) endures pre-emphasis process as a part, v(t) is passed through high pass filter to compensate and amplify the high frequency components of v(t) that is suppressed during recording of V_i.

$$\text{Emphasized\_signal} = \text{numpy.append}\{\text{signal}(0:) - \text{pre\_emphasis} * \text{signal}(:-1)\} \tag{5}$$

$$y(t) = v(t) - a * v(t-1) \tag{6}$$

$$y(t) = v(t) - 0.95 * v(t-1) \tag{7}$$

2) The value of filter coefficient (a) may be considered as 0.95 and y(t) is the pre-emphasis output whose output ranges between 0.9 to 1.
3) The v(t) is continuous and analog in nature and to segment the v(t) in discrete samples, the analog to digital conversion process (ADC) is executed to acquire speech samples of desired duration. In our system, the speech duration is fixed as 15 to 20 ms and v(t) is distributed into frames of N number of samples. The value of N may range from 128 samples to 512 samples. The values of M and N in this proposed system is considered to be 100 and 256 such that $M < N$.
4) To maintain the continuity of voice sample from first to last sample, the hamming window is multiplied with each 256 sampled and is represented as w(n), where

$$y(n) = v(n) * w(n) \tag{8}$$

$$w(n) = 0.54 - 0.46\cos\left\{\frac{2\pi n}{N-1}\right\}; \quad 0 \le n \le N-1 \tag{9}$$

Where, v(n) is input voice signal, y(n) represents output signal.
5) To endure N point (N may be 256 or 512) fast fourier transform, the V(t) has to be converted from time domain to frequency domain signal such that the algorithm depends on factorization of number of samples N.

$$Y(\omega) = FFT[h(t) * v(t)] = H(\omega) * v(\omega) \tag{10}$$

6) The h(t) and v(t) are the time domain signals is converted to frequency domain signals namely $H(\omega)$ and $v(\omega)$ by performing fast fourier transformation. The power spectrum of the signal is computed by

$$P = \frac{|FFT(v_i(n))|^2}{N}, \tag{11}$$

(Continued)

Table 4: Continued

Where the $v_i(n)$ is the "i^{th}" sample of input signal v(t).
7) The triangular filters will be relevant to compute filter banks with nfilt = 40 in the Mel scale to extract the frequency bands from power spectrum. The mel scale targets to impersonate the non-linear human ear perception for sound, by being lightly discriminative towards high frequency and heavily discriminative towards low frequency bands. The frequency (f) component can be converter to mel (m) component by

$$m = 2595\log_{10}\left(1 + \frac{f}{700}\right) \tag{12}$$

$$f = 700(10^{m/2595} - 1) \tag{13}$$

The summation of filter spectrum components yields the Mel (m) scale. In this proposed model, the mel(m) works out to Nfilter = 40 samples,

$$m = \sum_{j=1}^{N} f_c \tag{14}$$

Where, f_c is filter coefficient, and the mel coefficients for the sample voice print is

$$f_c = \{f_1, f_2, f_3, \ldots, f_N\} \tag{15}$$

$$m = \sum_{j=1}^{N} f_c = K_v \tag{16}$$

Where, K_v is the cumulative filter coefficient of the input speech signal
8) The frequency to mel scale conversion is done through

$$M(f) = 1125ln(1 + K_v/700) = V_a \tag{17}$$

9) The mel(m) spectrum is converted into time domain implementing discrete cosine transform (dct) to obtain Mel Frequency Ceptrum Coefficient. Each and every input sound sample is converted into a series of acoustic vector V_a
10) The session key from V_a are extracted through V_a = MFCC(dct).
11) The AS_i involves AES to decrypt M1 with key $K(IMSI_i \| h_i \| r_i \| SN_i)$ and rejects request if IMSI is not enrolled in DB_i.
12) The AS_i, if ($SN_j < SN_i$), computes $C_i = h(IMSI_i \| \gamma)$ and $h_i^* = h(C_i^* \| r_i \| SN_i \| IMSI_i)$ to check if $h_i^* ! = h_i$ to terminate process over authentication failure.
13) In case of $h_i^* ! \neq h_i$, choose r_j to compute $R = r_i \oplus r_j$ to generate Session Key $SK_i = h(IMSI_i \| r_i \| r_j \| C_i)$ and to compute $h2 = h(IMSI_i \| r_i \| r_j \| SN_i \| C_i \| SK_i)$.
14) The process conclude on the AES encryption of $\beta = Er_i(C_i)$ and sends $M2 = E_\beta(h2 \| R \| SN_j \| IMSI_i)$ to U_i through an open channel.

3.5 Algorithm for Session Key Generation

This phase involves U_i, AS_i and BS_i to issue secure session key based on successful verification of credentials as the process continuation to authentication checking of authorized U_i. The Fig. 4, depicts that the session key generation followed by the request for ticket by the user U_i to the bank server BS_i through authentication server AS_i. The bank server issues the session key on successful verification of authentication and the ticket is forwarded to user U_i through the authentication server AS_i.

On reception of message M2, the algorithm for session key generation is executed as per illustrated in Tab. 5.

Table 5: Algorithm for session key generation phase

Algorithm for session key generation phase
1) The U_i decrypts M2 on AES basis using $\beta = Er_i$ (C_i) and computes $r_j^* = R \oplus r_i$ to perform $SK_i^* = h(IMSI_i \| r_i \| r_j \| C_i)$ based on which to compute $h2^* = h(IMSI_i \| r_i \| r_j^* \| SN_i \| C_i \| SKi^*)$ to check whether $h2^*! = h2$. 2) The equality in h2 terminates the connection whereas the contrary relation assigns $SK_i^* = SK_i$ that issues session key between U_i and AS. 3) On reception of SK_i, the U_i performs AES encryption $F_i = E_{Ski}(IMSI_i \| BID_i)$ to send $M3 = (F_i \| h(IMSI_i \| BID_i))$ to AS_i through open channel. 4) The AS_i in turn decrypts $(IMSI_i \| BID_i) = D_{Ski}(Fi)$ to compute and check $h^*! = h(IMSI_i \| BID_i)$ leads to termination and rejection of login process, whereas the $h^*! \neq h(IMSI_i \| BID_i)$ proceeds in obtaining IP address (IP_i) of BS_i to send $(M4 \| h(PID \| N1)$ to BS_i in open channel by choosing a N1 and encrypting $M4 = E_{Ki}(PID \| N1)$. 5) The BS_i computes h^* by decrypting M4 to generate $(PID \| N1)$ and $h^*! = h(PID \| N1)$ terminates the ticket granting process while $h^*! \neq h(PID \| N1)$ generates N2 to compute session key (SKAS), $SKAS = h(N1 \| N2 \| PID \| BID_i)$ such as to AES encrypt the M5 $= E_K((PID \| N1 \| BID_i \| N2 \| SKAS)$ to AS_i over an insecure channel. The AS_i decrypts $D_K(M5)$ to attain $(PID \| N1 \| BID_i \| N2 \| SKAS)$ to compute and check $h(PID \| N1 \| BID_i \| N2)$ with SKAS, such that the equality leads to termination of session while the contradictory progress to follow AES encryption of $M6 = E_{SKAS}(BID_i \| N2)$ to requested U_i by way of an insecure channel.

3.6 Algorithm for Shielded Transaction Phase

This phase involves U_i and BS_i to perform a shielded transaction between the U_i and BS_i as the session key is issued and confirmed to grant a secure transaction. The Fig. 5, illustrates the shielded transaction between the user U_i and banking server BS_i. The user U_i sends the fingerprint minutiae to the banking server and on successful verification the shielded transaction is granted to the user U_i.

1) The U_i on applying the unique FP_i extracts the features FP_i = Minutiae ( ) to encrypt $MSG = E_{vi}(FP_i \| N1 \| E_{SKAS}(BID_i \| N2))$ to BSi.
2) The BS_i decrypts $D_{key}(MSG)$ to acquire $(FP_i \| N1 \| E_{SKAS}(BID_i \| N2)$ and $D_{SKAS}(E_{SKAS}(BID_i \| N2)$ to test BID_i ! = BID_i and N2! = N2 leads to termination of transaction while

the amend leads to establishment of session and extraction of N1 to execute a successful transaction in triumph of $FP_i == FP_i^*$.

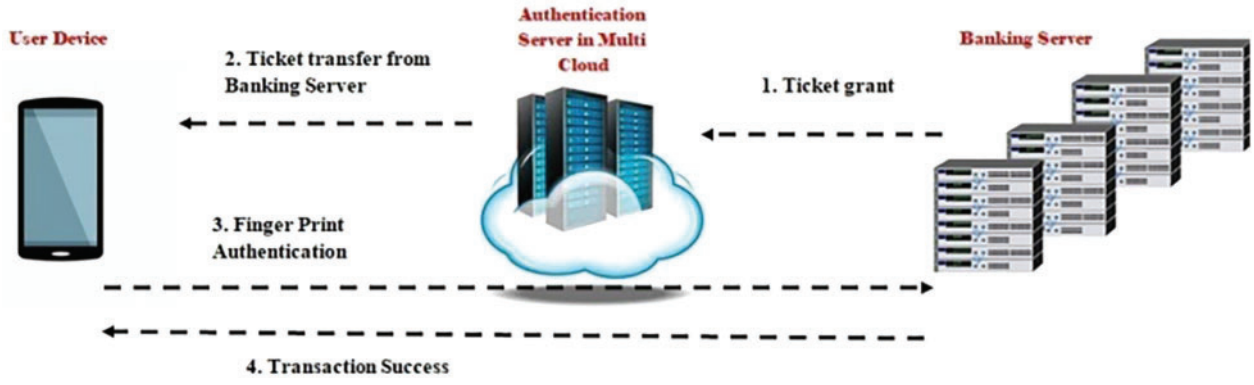

Figure 5: Message flow diagram- shielded transaction phase

On successful clearance of authentication process, the authentication server connects the user device with banking server to perform the transaction in a shielded mode.

4 Security Analysis

We put forward that our proposed model has much merits and can defy multiple security threats.

4.1 Theorem 1. The Proposed Model Provides Tough Anonymity Against Man-in-the-Middle Attack

Proof: This type of attack, the attacker attempts to alter the communication between U_i, AS_i and BS_i. In this case, the proposed system is resistive against this attack as the key q, K_1, K_2 were generated in offline mode. The $IMSI_i$ identity acts as a key to receive information from AS_i and BS_i which is unique and is stored in DB_i of AS_i in offline mode. Hence the possibility of extracting the $IMSI_i$ information is very low in this system. Also the AS_i sends $\{\alpha, B_i, D_i, SN_i\}$ over offline mode, even on breaking this information, the attacker feels hard to crack the information as the p_i is private to the U_i. The threat to M1-M6 were decrypted with $\{K, B_i, D_i, SN_i\}$ were stored in U_i resists the attack hardly and has a least probability of success in attack.

The message M1: $M_1 = E_K(IMSI_i \| h_i \| r_i \| SN_i)$; M2: $M2 = E_\beta(h2 \| R \| SN_j \| IMSI_i)$; M3: $M3 = (Fi \| h(IMSIi \| BIDi))$; M4:$M4 = E_{Ki}(PID \| N1)$; M5: $M5 = E_K((PID \| N1 \| BID_i \| N2 \| SKAS)$; M6: $M6 = E_{SKAS}(BID_i \| N2)$.

Let we consider, that hacker tends to know the $IMSI_i$ of user U_i, and the entire message content through the successful execution of Man in the Middle attack, the hacker needs to know the key "k, β" which were the private keys generated by the AS_i for BS_i and User device U_i.

4.2 Theorem 2. The Proposed Model Withstands Stolen Sim-Card Attack

Proof: The U_i stores the confidential information $\{K, B_i, D_i, SN_i\}$ vital for decryption of M1-M6 face a threat of data disclosure on stolen sim card attack. Any attacker on having the confidential stored information and the sim card can involve in man-in-the-middle attack. The proposed model highly withstands stolen sim card attack, as the SK_i is generated on verification

of V_i extracted from V_u which is unique to each user. Without generation of SK_i, the stolen sim card and details have no more active in associative with the actions of attacker. Furthermore, SN_i is invalidated without V_i = MFCC(dct) and this system is invulnerable to stolen sim card attack.

Consider the user device U_i has been lost or stolen by hacker to have an authorized access by an unauthorized user using the device U_i and with $IMSI_i$.

M1: $M_1 = E_K(IMSI_i||h_i||r_i||SN_i)$; M2: $M2 = E_\beta(h2||R||SN_j||IMSI_i)$; M3: M3 = (Fi||h(IMSIi||BIDi));

M4: $M4 = E_{Ki}(PID||N1)$; M5: $M5 = E_K((PID||N1||BID_i||N2||SKAS)$; M6: $M6 = E_{SKAS}(BID_i||N2)$.

The hacker, knowing the $IMSI_i$ information is not sufficient to gain the session key illegally as he need to know the other parameters like.

4.3 Theorem 3. The Proposed Model Provides Rigid Secrecy Against Password Guessing Attack

Proof: In this type of attack, the attacker employs cryptanalytic techniques and attempts all probabilities of password against PW_i. The attacker gains PW_i related information from DB_i for the successful guessing of exact PW_i but cannot be able to identify the decryption keys {K, B_i, D_i, SN_i} which was shared offline among U_i and AS_i. The proposed system involves {PW_i, V_i, FP_i} for successful authentication whereas the later two credentials is highly essential for generating and sharing of SK_i. The {V_i, FP_i} and biometric sets that are not available in any directories. Thus the attacker even though succeeded in password guessing was blind in {V_i, FP_i} flops in generation of SK_i that proves the proposed system is highly resistive to password guessing attack.

Consider the hacker succeeds in guessing the low entropy password of User U_i.

M1: $M_1 = E_K(IMSI_i||h_i||r_i||SN_i)$; M2: $M2 = E_\beta(h2||R||SN_j||IMSI_i)$; M3: M3 = (Fi||h(IMSIi||BIDi));

M4: $M4 = E_{Ki}(PID||N1)$; M5: $M5 = E_K((PID||N1||BID_i||N2||SKAS)$; M6: $M6 = E_{SKAS}(BID_i||N2)$,

The hacker fails in decrypting any of message M1-M6 as it needs information about SN_i, BID_i, PID, SKAS which still a short fall for the hacker to succeed in gaining unauthorized access.

4.4 Theorem 4. The Proposed Model Counters Known-Key Attack

Proof: Let's consider that the attacker hacks the session key, tends to acquire the session illegally leads to failure attempt. The system proves to be rigid against any sort of attacks as the authentication process relies on multiple keys {γ, p_i, K_1; K_2, K_3} and is still secure that the final access grant relies on user's voice print V_i and finger print FP_i. The fact that the attacker manages to know the key value, the proposed model not only relies on cryptographic keys but also utilize PW_i, V_i = MFCC(dct) and Finger print FP_i = Minutiae( ). These credentials are essential for the computation and grant of SK_i to the known U_i. Hence the proposed model is highly rigid towards the known key attack.

M1: $M_1 = E_K(IMSI_i||h_i||r_i||SN_i)$; M2: $M2 = E_\beta(h2||R||SN_j||IMSI_i)$; M3: M3 = (Fi||h(IMSIi||BIDi));

M4: $M4 = E_{Ki}(PID||N1)$; M5: $M5 = E_K((PID||N1||BID_i||N2||SKAS)$; M6: $M6 = E_{SKAS}(BID_i||N2)$

Let us consider the hacker encounters with known key attack and is aware of secret keys k, β and can decrypt the message M1 to obtain the session number SN_i . To obtain SN_i, the user has to undergo successful authentication check with low entropy password, $IMSI_i$ and minutiae matching confirmation process. Hence the known key attack proves to be insufficient to gain the illegal access of session key SK_i.

4.5 Theorem 5. The Proposed Model Discards Parallel Session Attack and Insider Attack

Proof: The Parallel session attack and the Insider attack in the cloud environment is, the attacker tends to grab the session illegally by gaining information about the keys $\{\gamma, p_i, K_1; K_2, K_3\}$. The proposed model engross $\{\alpha, B_i, D_i, SN_i\}$ keys which are computed within U_i and were shared in offline mode, which the parallel session attacker is not aware of remains fail in decrypting ((PID‖N1‖BID_i‖N2‖SKAS)) and gaining the session to perform transaction. Hence the proposed system discards the parallel session attack and insider attack.

4.6 Theorem 6. The Proposed Model Rebuff Denial of Service (DoS) Attack

Proof: The attacker introduce Denial of service attack in the cloud environment to make the service unavailable to the U_i by flooding the target network with superfluous traffic intends to overload the network. The proposed model is highly resistive to this attack, the AS_i exercise N1, N2 value which were time bounded. The session establishment SK_i transmits ((PID‖N1‖BID_i‖N2‖SKAS)) and the N1 and N2 were time bounded exceeding which the transaction is terminated. Thus the proposed model strongly rebuffs the denial of service attack.

M1: $M_1 = E_K(IMSI_i‖h_i‖r_i‖SN_i)$; M2: $M2 = E_\beta(h2‖R‖SN_j‖IMSI_i)$; M3: M3 = (Fi‖h(IMSIi‖BIDi));

M4: $M4 = E_{Ki}(PID‖N1)$; M5: $M5 = E_K((PID‖N1‖BID_i‖N2‖SKAS)$; M6: $M6 = E_{SKAS}(BID_i‖N2)$

The Denial of Service (DoS) attack proves to be unsuccessful as the half completed request will exhaust due to the nonce value encrypted in all message M1-M6.

4.7 Theorem 7. The Proposed Model Proves Rigid Against Authentication Server Attack or MITC Attack

Proof: The attacker tends to attack the authentication server AS_i rather than performing other attacks to gain illegal access of a single user. The authentication server attack on becoming success, ease the attacker to gain the access of all the sessions that the authentication server acts as gateway. The proposed model proves highly rigid against the authentication server attack or insider attack as the system possess multi factor authentication system that includes low entropy password, feature extracted from voice print, IMSI identity of authenticated user's device and user finger print noted as $\{PW_i, V_i, IMSI_i, FP_i\}$. The attacker in the authentication server AS_i may illegally gain information of $\{PW_i, V_i, IMSI_i\}$ as all these secure credentials were verified and communicated through authentication server which is already compromised. The user's finger print FP_i is the final authentication credential that is passed over channel directly to banking server BS_i where the MiTC attack proves inefficient in gaining the fingerprint FP_i information.

5 System Evaluation

In this section, we analyzed the proposed system in terms of efficiency and effectiveness based on the key size and strength. The parameters considered for the analysis are the length of $IMSI_i$, length of low entropy password PW_i, random numbers and message digest M1-M6 against computing time represented in milli seconds. We had chosen key words of multiple lengths ranges from 160–512 bits to perform the experiment of measuring the efficiency of our proposed system. The Fig. 6 illustrates the response of computational time with respect to the key length in bits. For clarity, the $IMSI_i$, random numbers were numerical value whereas the PW_i is composed of alphanumerical and special characters. To calculate the actual key length, we convert the key to

numerical format as follows

$$W = \sum_{i=1}^{Length(PW_i)} ASCII(PW_i) \tag{18}$$

The weight of PW_i created by the U_i is determined by converting the PW_i into an equivalent ASCII code. From Fig. 6, it is evident that the increase in key length directly drives computational time proportionally and to achieve a least computational time the summation of key length of PW_i, r_i, r_i, messages (M1-M6) must be short that attenuates the strong security against various attacks.

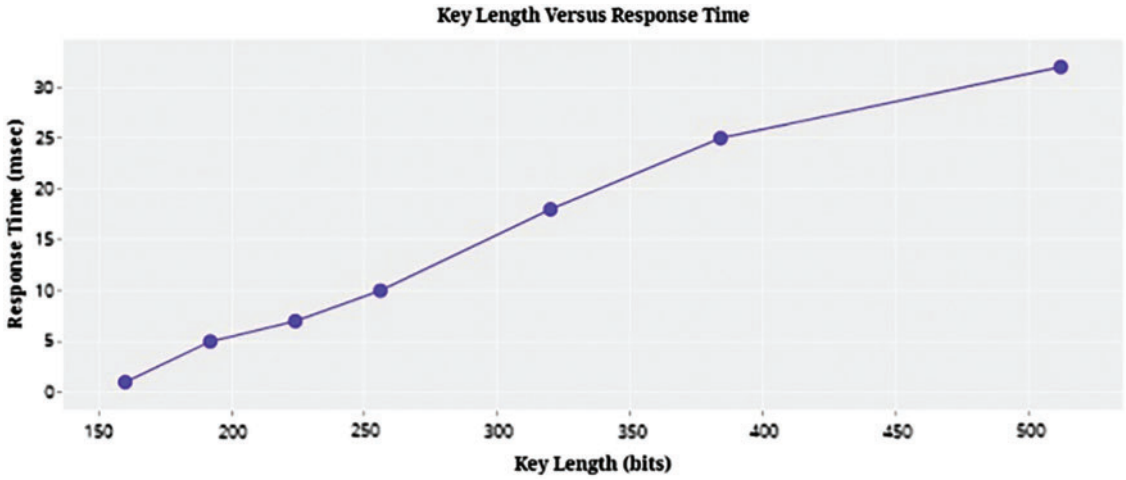

Figure 6: Comparison of key length with computation time

It is reasonable to select PW_i, r_i, r_i, M1-M6 of average length means neither short nor too long such that to achieve computational time at customary range. In our proposed model, we chose the key length to be 256 bits based on outcome of system analysis. The computation time in the proposed system is classified into three phases namely user login phase, AS_i authentication phase and BS_i authentication phase. The proposed system transmits {M1, M2, M3, M4, M5, M6} between the entities to authenticate the user and this message is of {1024 + 1024 + 128 + 128 + 1024 + 128} = 3456 bits which is lesser when compared to the reference model considered in this system. This makes the system to compute faster and to authenticate the user at faster rate such that it is more secured as it consumes least time which is not sufficient for any hacker to perform brute force attack. The proposed system provides high level of security as it involves user's unique biometric identities namely user voice coefficient and fingerprint along with the low entropy password to authenticate the right user.

As explained earlier, the MFCC algorithm employed here performs hamming window to extract the Mel frequency coefficients from unique voice sample V_i which has high response towards all range of frequencies. The Fig. 7 depicts the feature point extraction from the voice print V_u. The hamming window detects and corrects the discontinuities in the start and end of voice sample to obtain the accurate Mel coefficients from the V_i.

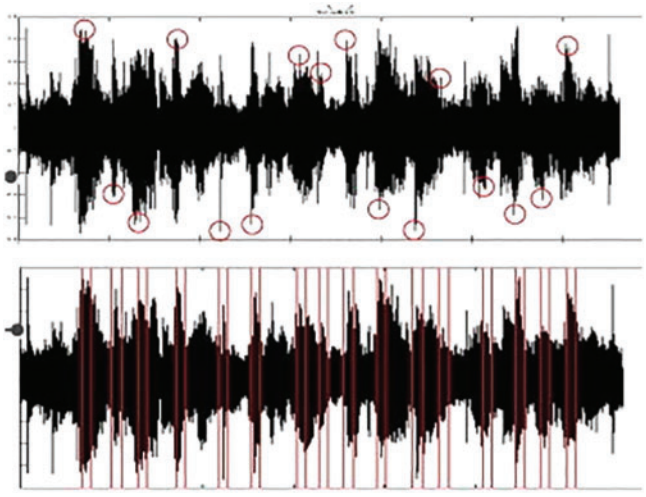

Figure 7: MFCC feature point extraction

In the proposed system, the nonce period is 60 s and from the Fig. 8, it is clear that the proposed system utilize maximum of 12 s to respond for 1000 user requests. Hence the proposed system is proven to be highly robust against Denial of Service attack.

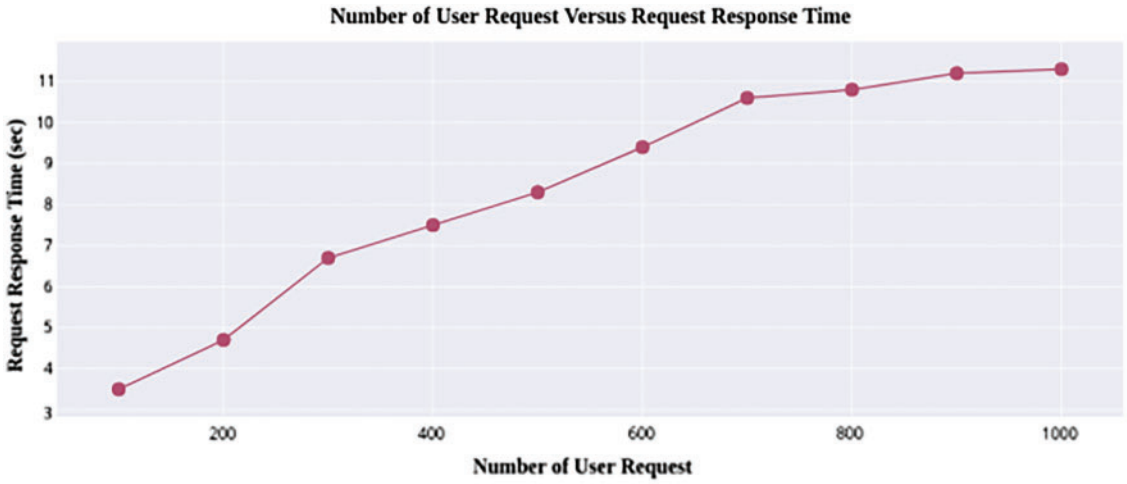

Figure 8: Comparison of number of user request with request response time

6 Conclusion

The authentication verification and secured transmission in the cloud network is a biggest challenge for which our proposed model, identity based secured transmission using MFCC algorithm provides better results and withstand various types of attacks in cloud environment. Our proposed system is efficient that proves its rigidity against any attacks and afford secured session key and mutual authentication to perform secure transmission over insecure network. As the protocol provides session key security, this protocol supports efficient practical applications in cloud network. The system has a capability of enhancing the security feature by safeguarding

the credentials in authentication server database DB_i be the future development to provide strong protection against any attack in particular the Man in the Cloud (MiTC) attack.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Lula, O.Dospinescu, D. Homocianu and N. A. Sireteanu, "An advanced analysis of cloud computing concepts based on the computer science ontology," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2425–2443, 2021.

[2] Y. Ren, C. Wang, Y. Chen, M. C. Chuah and J. Yang, "Signature verification using critical segments for securing mobile transactions," *IEEE Transactions on Mobile Computing*, vol. 19, no. 3, pp. 724–739, 2020.

[3] J. Luna, A. Taha, R. Trapero and N. Suri, "Quantitative reasoning about cloud security using service level agreements," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 457–471, 2017.

[4] 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.

[5] P. N. Brown, H. P. Borowski and J. R. Marden, "Security against impersonation attacks in distributed systems," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 1, pp. 440–450, 2019.

[6] Q. Hu, B. Du, K. Markantonakis and G. P. Hancke, "A session hijacking attack against a device-assisted physical-layer key agreement," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 691–702, 2020.

[7] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu *et al.*, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2519–2533, 2015.

[8] Y. Han, L. Duan and R. Zhang, "Jamming-assisted eavesdropping over parallel fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2486–2499, 2019.

[9] K. Fan, H. Li, W. Jiang, C. Xiao and Y. Yang, "Secure authentication protocol for mobile payment," *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 610–620, 2018.

[10] R. Garg, M. Gupta, R. Amin, K. Patel, S. H. Islam *et al.*, "Design of secure authentication protocol in socks V5 for VPN using mobile phone," in *Int. Conf. on Trends in Automation, Communications and Computing Technology*, Bangalore, India, pp. 1–6, 2015.

[11] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen *et al.*, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1382–1392, 2017.

[12] J. Soares and A. N. Gaikwad, "Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP," in *Int. Conf. on Automatic Control and Dynamic Optimization Techniques*, Pune, India, pp. 409–414, 2016.

[13] S. K. Hafizul Islam, G. P. Biswas and K. K. Raymond Choo, "Cryptanalysis of an improved smartcard based remote password authentication scheme," *International Journal for Information Sciences*, vol. 3, no. 1, pp. 35–40, 2014.

[14] Q. Tao and R. Veldhuis, "Biometric authentication system on mobile personal devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 763–773, 2010.

[15] C. Preethi and H. Om, "Cryptanalysis and extended three-factor remote user authentication scheme in multi-server environment," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 765–786, 2017.

[16] 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.

[17] W. Pan, F. Zheng, Y. Zhao, W. Zhu and J. Jing, "An efficient elliptic curve cryptography signature server with gpu acceleration," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 111–122, 2017.

[18] J. Jensen and Z. Tan, "Minimum mean-square error estimation of Mel-frequency cepstral features—A theoretically consistent approach," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 23, no. 1, pp. 186–197, 2015.

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