International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Improvised Multi-Factor Authentication for End-User Security in Cyber Physical System

M.Maranco[1]*. R.Logeshwari[2]. M.Sivakumar[3]. V.Manikandan[4]

Submitted: 08/12/2023 **Revised:** 18/01/2024 **Accepted:** 28/01/2024

Abstract: End-user security is the most important thing in day-to-day life. We use a security system for household appliances, vehicles, smartphones, etc., to protect and safeguard our things and the environment. The Cyber Physical System (CPS) contains an internet-enabled digital component. CPS security is applied in many areas, such as transport, healthcare, and all industry 4.0 applications. Multi-Factor Authentication (MFA) is one of the traditional authentications that helps enhance the security level in CPS. The typical authentication method contains a strong password, biometrics, etc. Even though the current end-user security system has implemented a legacy digital control mechanism, the system has a higher chance of getting compromised through malicious activities. The major point of the MFA approach is that intruders can be blocked at any level of the authentication scheme. This study aims at developing a secure and efficient authentication gateway. The proposed system presents enhancements to end-user security using MFA techniques. Three distinct works in this study use MFA technique. The MFA technique consists of three distinct layers. The end-user's geo-location is considered the first security gateway by the user distance within the range of CPS and validates the user's current position with predefined geo-location logic. One Time Password (OTP) send through e-mail is used for the second layer. Hash algorithms such as SHA256 or SALTING use the third layer implementation. The typical CPS needs to authorize and authenticate the user's identity to ensure end-users identification in the modern security system. Efficient and secure multi-factor authentication techniques designed and evaluated on end-user digital health applications and obtained the results with the accuracy of 95.50%, 97.50% and 96.40% respect to three distinct layer authentications. The developed system also analyzed the formal and informal verifications against to the various attacks.

Keywords: *Multi-Factor Authentication· One Time Password· Geo-location· Cyber Physical System· e-health environment*

1. Introduction

The main objective of this work is to use various security methods to defend the current condition. However, due to current hospitals' incredibly low rates of security betrayal, the transaction is either indirect or direct. The anticipated cost of a data breach in 2019 was $3.92 million, while the cost to the health care environment as a result of the violation was $6.45 million, according to the International Business achiness (I.B.A.) survey. According to the Clearwater Cyber Intelligence Institute, user authentication is the most common and vulnerable cybercrime for the hospital and the healthcare system. Authentication of multi-tier level network security has been proposed in these processes.

The methodology of the existing security has been improved by the work done with it. To access the easy reduction, this has the possibility to allow any account. The user's account and the medical database were among the connection of the particle. Using the traditional algorithm for a long time, the security adequate was too difficult, and the cryptonym was in high progress based on the advancement of the recent year [1-3].

The computing cloud with different and challenging with quite an authentication. The financial transactions, the security transaction which has been carried that has been required based on the security information. The parameter of the authentication was included individually based on the online financial transaction and the information based on the related account. All the communication entities were identified, which has been corrected based on the key techniques of the scheme authentication. In the data storage, the data were authorized only by the user. At the database, the data has been kept by the user hesitates, provided by the third party. The resources, the permission of seeking the valid person were started identified by some data resources. In the medical sector, the encryption and the cryptographic algorithm were more secure with the transmission, which has been improved, based on the work. The existing method was based on the medical sector [4,5]. The password and the user name that validated based on the hasting technique of Secure Hash Algorithm 2 (SHA 2) in order to provide the security strategies that have been enhanced and the performances of the highest hashing algorithm for the services of the transaction data [4-8].

The working principles of the security system with Firebase Real-time database architecture are shown in Fig.1.

[1,2,3]*Department of Networking and Communications, Faculty of Engineering and Technology, SRM Institute of Science and Technology,Kattankulathur, Tamilnadu, India*
[4]*Department of Electrical and Electronics Engineering, Coimbatore Institute of Technology,Coimbatore, India.Email:rloge29@gmail.com*

** Corresponding Author Email: maranco.m.phd@gmail.com*

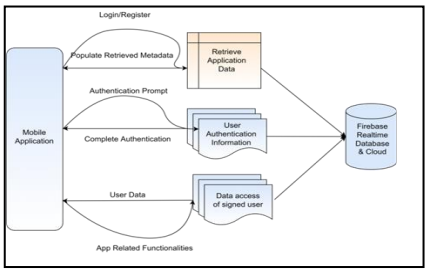

Fig.1 Firebase Real-time Database Architecture

This paper is structured as follows: Section 2 gives background work on the multi-factor authentication and cyber physical system assessment. Section 3 contains a methodology explaining the experimental procedure and authentication factors developed with the unique techniques. In Section 4, the results obtained with the proposed method are explained. The conclusion remarks have discussed in Section 6.

1.1. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have already been defined in the abstract. Abbreviations such as IEEE, SI, ac, and dc do not have to be defined. Abbreviations that incorporate periods should not have spaces: write “C.N.R.S.,” not “C. N. R. S.” Do not use abbreviations in the title unless they are unavoidable (for example, “IEEE” in the title of this article).

2. RELATED WORKS

The user's location that the next authentication factor has used. In this application, the account that contains the access based on the location of three different places limits the user based on the security level that enhanced. During the registration/sign up, the user access the system, which can be chosen and fed originally from the location. The breach possibility has the elimination of factor for an unknown location. During the registration, the excellent location selection within a radius of 2 km were application that has been login that can attempt the user. The current location of the user tracks down easily and within the system of the location of GPS by having the modern mobile phone of all the specifications based on the external hardware without any possibility that has been made the user's longitudinal and latitudinal location has been tracked down by using the API Google system location. During the login, the user's location can be pre-defined in 3 points. This one location is the present location of the user. The factor authentication will pass his/her location. If the user can access different location, it will deny access to the user, and the message alert or security will be sent to the user's mail and mobile phone. The access control and authentication have been efficient based on the user mechanism with the security existing from the location information integrated from the mobile device GPS [9-16].The user, the authentication, the user an OTP method, and the OTP (One Time Password) were sent via e-mail to the registered account to login to the user account. When a user needs to authenticate on a device, the server sends the user an e-mail containing the OTP required to log on to their account. This OTP can be utilized for a short, predetermined period during a single authentication. The OTP was produced by the server based on the user's location coordinates when logging into the account or doing any other action. While compared to mobile OTP, the E-mail OTP is significantly safer than the risk associated with receiving an OTP by SMS because anybody can call the phone company, and the number can be forwarded to any mobile device [18].The victim's cell phone was provided, and the attacker assumed the number. When the phone number changes, it is impossible to limit the possibility that the sender's OTP will not be updated. Moreover, secure the approach by instantly changing the phone number when the victim may not be aware of the changes. The SMS OTP can be hacked. Thus, it is secure to transmit the OTP over the mail. Nowadays, all mail contains its 2FA, and it is extremely secure. In this authentication scheme, the e-mail OTP is employed as the factor [17-26].

The channel communication security depends on the 2FA security, the second factor for the integrity and transmitting OTP from the user. These assumptions were ensured based on the 2FA failure in sending the SMS and the 2FS user despite the account login due to the attack in the past. To receive the OTP through the SMS, the attacker cannot attack the SI port, which was stolen in the bitcoins wallet in May 2019 (https://link.medium.com/udDy3fGLQW).

The provided popular services across the authentication that spread two-factor to analyze the speed. The data specific that obtain the list is to possible reproducible of being the offers the advantage that offer. The 57 unique login is identified the 75 domains. Representing the login and registration with the website that we found the domain 100 analysis. By enabling the 2FA to secure the account that allows the user, we found the 57-domain analyser [22-26].

The user's web authentication is the most widespread practice, but passwords have a poor reputation among security professionals. The infrastructure of the cumbersome alternative must be maintained and deployed. Information that becomes the computer's protective technology is stored in the paper document's database. The collision and pre-image attacks could withstand the hash function's resistance. In many cases involving random numbers, a computer application may be required. The cryptographic key or password's potential to circumvent the one common method was the application of cryptographic evasion. The security of the system was circumvented to exploit a vulnerability that could be exploited by a hostile agent when generating the password that has been employed by the random number generator [4].

The technique that is most popular in authentication is the password. By using the SHA-2 Algorithm, the user password includes the hashing factor. The password can be in the form of any special series of characteristics, numbers, or letter format. The password should be strong and contain all availability of mixer choices to self-secure one. Grooming poor and phishing attacks are vulnerable through the password, which may perform weakly. However, based on the user's viewpoint, the method should be effective and easy to prove. Therefore, to make the password difficult to use, to achieve the aim that we are processing. To keep the data secure, they design a cryptographic family function based on the secure hash algorithm they know as SHA. To transform the data by using a hash function, it operates. The operation of bitwise considers an algorithm with compression function and additional modular. By hash function, they generate the original that looks like nothing for the fixed-size string. They are the one-way function designed based on the Algorithm. The hash values were respective into their converted that once ensured it, to the original data back from the convert back from the nearly impossible value. The Algorithm used in the notes was SHA-1, SHA-2, and SHA-3; they built-in the reaction

that was successive with each other to strengthen the encryption to progress with the assault of the hacker. A false certificate can be created and mounted by the attacker, which can be manipulated by the user of SHA-1 based on enough computation resources. The two main reasons for the time over the efficiency less to get the levels of security typically. For the attacks computer challenge, they practice more to make more power for processing the declining cost. With no collision records, the method of secure hashing was provided with SHA-2 [4-8].

Real-time databases are a hallmark of cloud-hosted databases. The data storage in JSON was continually synchronized with each client association. A large portion of users depends on the insurance of the majority when an application is designed cross-platform using JavaScript, Android, SDK, and iOS, based on the Real-Time Database. A database was created to avoid a process that emerged with the allowed functionality, and Firebase primarily managed the back-end application. The information can be finely created or browsed when presented as the database that should be arranged and defined by the language of expression-based rules. Building a portable that has been used for the firebase framework and in the database record based on the user update has implied basing the Real-Time Database that is utilized for the company's web application, the imparted update to the instantly every user. The service is contained in the feature host's packet and the cross-platform application. The built application is delivered over a side server that Firebase can manage. Depending on the developer's point of view, which has been produced using the tool developed with Firebase by many elements. The client and developer can retain their harmonious relationship by delaying work as little as possible [29,30].

2.1. Research Gap on the existing literature

From the existing literature, it is found that the location-based authentication was not carried out and timestamp information was not considered on the end user authentication system. It is also noted that when the number of user increased, the performance of the proposed framework degrades. To address these issues, the current manuscript enhances the end-user security using Multi-Factor Authentication (MFA).

2.2 Contributions

The contributions of the Multi-Factor Authentication for end-user security in cyber physical system as follows:

- The location-based authentication used as a one factor was considered to treat distinct and precious geographical locations by haversine logic.
- The current trends were also considered on Multi-layer authentications to enhance security level. The second factor was implemented using mail OTP.
- Salting and Hashing were applied for third factor authentication. These all three factors taken as Multi-Factor Authentication for end-user security.
- A hybrid authentication model was constructed for end-user security system using Multi-Factor Authentication (MFA), and then the proposed model was experimented on five scale of users: 1-10, 11-20, 21-30, 31-40, 41-50 better accuracy of 98.90%, 98.85%, 98.70%, 98.60%, and 98.50% respectively.

3. Preliminaries

The implementation is done in two phases, Sign Up and Sign In. The steps involved in each phase are listed below:

3.1 Registration Phase

The following steps are involved for the sign-up phase:

Step1	The user enters mail ID
Step2	Mail verification link is sent to the provided mail ID. To verify the mail, the user must click the link that was sent.
Step3	The system prompts the user to provide a password. The password is to be chosen in such a way that it meets the strong password requirements specified.
Step4	Password is appended with salt, hashed using SHA-256 and stored in the database. The salt is also recorded.
Step5	The user chooses three locations in which he/she is likely to access the application.
Step6	The locations' coordinates are picked and stored in the database for verification purposes.
Step7	The user is redirected to the Sign In phase after completing the 6th step.

3.2 Sign-in Phase

The following steps are involved in the sign up phase

Step1	User enters mail ID
Step2	User's current location is captured. The locations given by the user during Sign Up phase are retrieved and checked against the current location to see if the user is within the 2km radius of any of the provided locations.
Step3	Upon successful location verification, an OTP is sent to the user's mail ID, which expires within a specific amount of time.
Step4	User enters the OTP sent to move to the next authentication factor.
Step5	User enters password. The hashed password of the user and salt are retrieved from the database. The password provided by the user is hashed after appending the salt and is checked with the hashed password retrieved from the database.
Step6	User is granted access to the application upon completing the above steps.

4. Proposed Methodology

The proposed end-user security using Multi-Factor Authentication (MFA) shown in Fig.2. The MFA consist of three distinct factor implemented as follows.

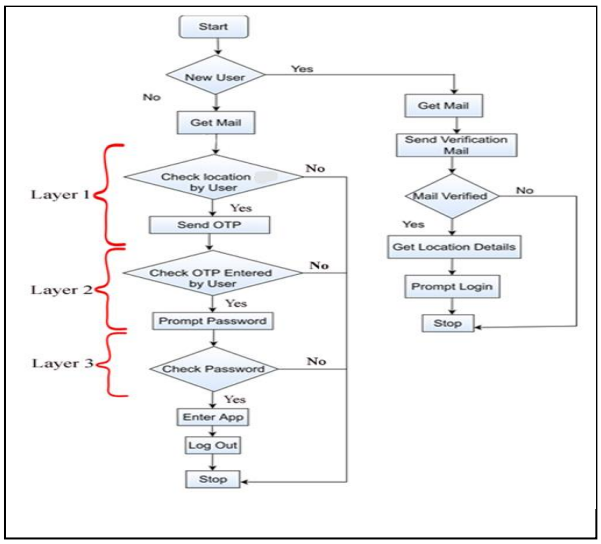

Fig.2 MFA Flow diagram

4.1 Factor 1 - Location Authentication

The Haversine formula determines the sphere with the two locations between the great circle's distances by its latitude and longitude. The spherical triangle is related with the harvesting law with the angle in spherical trigonometry, the most common formula employed in the unique situation with substantial

navigation.In 1805 James Andrew introduced the first table Haversine, but in 1801 Jose de Mendoza y Rios attributes the Florian Cajori. The term "HARVERSINE" is first used by James Inman in 1835.From the fact they derive the name, the haversine operation was based on the fact usually written, haversine provided through (θ) = sin2 (θ/2).Let (Θ) represents two points in a sphere with a mid or central angle:
where,

- The two points with the dimple distances between them i.e. the sphere with a great circle, see the distances of the sphere.
- Sphere radius that r indicates

Following the haversine formula that we have

$$HAV(\Theta) = \text{hav}(\varphi 2 - \varphi 1) + \cos(\varphi 1)\cos(\varphi 2)\,\text{hav}(\lambda 1 - \lambda 2) \quad (1)$$

Here,

- φ1 denotes point 1 latitude, whereas φ2 represents point 2 latitude
- λ1 denotes point 1 longitude, whereas λ2 denotes point 2 longitude.
- Finally, the haversine formula (half a versine) of an angle θ (used above-mentioned differences in latitude and longitude) is:

$$\text{Hav}(\theta) = \text{sin2}\left(\frac{\theta}{2}\right) = \left(1 - \frac{\cos\left(\frac{\theta}{2}\right)}{2}\right) \quad (2)$$

To address the distanced, use inverse haversine have-1 for the central angle Θ or use the arcsine (inverse sine) function:

$$d = r\,\text{hav} - 1\,(h) = 2r\,\text{arcsine}\,(\sqrt{h}) \quad (3)$$

here,

$$h = \text{hav}(\theta) \quad (4)$$

To substitute (4) into (3)

$$d = 2r\,\text{arcsine}\,(\sqrt{\text{hav}(\Theta)}) \quad (5)$$

To substitute (1) into (5)

$$d = 2r\,\text{arcsin}\,(\sqrt{\text{hav}\,(\varphi 2 - \varphi 1 + \cos(\varphi 1) + \cos(\varphi 2)\,\text{Hav}(\lambda 2 - \lambda 1))}) \quad (6)$$

To substitute (2) into (6)

$$d = 2r\,\text{arcsin}\,(\sqrt{\text{sin2}\left(\frac{\varphi 2 - \varphi 1}{2}\right) + \cos(\varphi 1)\cos(\varphi 2)\text{sin2}(\lambda 2 - \lambda 1))}) \quad (7)$$

When the user opens the app, the registration process takes place by the user, and at that time, they will choose three different locations; when the user is present or login the app at any time or place, the location that the user sets will be the location shown to others who will search or hack the device. With the coordinate helper, the database can be stored in our location. Within a radius of 2km, the user can choose the location where the user is currently available. In using the mail, the user must check the mail involved in the login procedure. When they enter the mail, this helps fetch the current user's location. By using their mail ID, they can also retrieve the registration of the user location during the time of it. Then the user's location is compared with the location of a 2km radius. The first-factor authentication is passed by the user successfully, the radius that specifies the inside of the user. The location specified with the three locations outside the user location, the screen login to back the app redirected. The app tries to login to alert the security as a mail to the user's notice. If login to anyone else other than the user, the account is secure, and the credentials to change the user to enable that would alert the login. The entire process of location verification is shown in Pseudocode 4.1

Pseudocode Location Verification

Begin
Function locCheck
get the user's mail
retrieve the user's unique key
If GPS permission not yet given to the application **Then** ask for GPS access permission from user
End If
If GPS not enabled Then
prompt user to enable GPS
End If
get the user's current location in coordinates
retrieve the user has selected 3 locations
If the distance between the current and selected locations is within 2km radius, **Then**
proceed to next module (pass user's key)
End If
Else
show message that user is outside the selected locations
End

4.2 Factor 2 - Mail OTP

This Multi-Factor Authentication is a factor that would be the second factor by an authentication mail. The user act as a primary username, which is the mail id to enter to promote the user during registration. The Random Number Generator (RNG) facilitates in the creation of numerous symbol arrays. A decent random option is not more predictable than it. Pseudo-random number generators or real number random assisted me in developing the actual HRNG (hardware random number generators) that could be RNG.

$$\text{OTP} = \boldsymbol{r} + \boldsymbol{e}\text{Mod Len} \quad (8)$$

Where,

r – random () using Random numbers
e – External Values
len – Length of the Alphanumeric

When the mail is entered for a specific mail ID, a verification mail will be sent to ensure the user can access the existence of the mail and the app. To complete the process, the verification link in the mail should be clicked by the user for the verification process. After some specific time, the link that is sent for the verification expires. The e-mail is verified, and the app will proceed with the next step to verify the user to complete the registration process. The user's details will be collected in this process of authentication. Next time the user tries to log in, the authentication factor is passed by the user, that is, authentication location, generation of OTP, and to the given mail ID, the mail has been sent. The OTP sent to the required mail ID will be received in the app where the OTP prompt is shown. The OTP that was entered matches the OTP that was sent to the mail. After that, the password verification will be directed to the user, which will be the final verification process in the authentication process. If an incorrect OTP is entered, the user will be sent back to the login page, and the user to begin the process from the start. The user receives a mail due to the failed login process. The entire

process of mail OTP verification is shown in Pseudocode 4.2.

Pseudocode Mail OTP Verification

```
Begin
    Function sendOTP
    instantiate a session from SMTP host with SSL socket with the credentials of the
    mail created for the application.
    OTP = Generate randomized 6 digit OTP
    include the OTP with the mail body and send the mail
        If verifyOTP( OTP ) Then
          proceed to next module ( pass  user's key )
        Else show message that OTP entered is wrong
        exit the application
        End If
    End Function
    Function verifyOTP(otp )
    get OTP entered by the user
        If OTP entered is equal to otp sent
          return True
        Else return False
        End Function
End
```

4.3 Factor 3 - Salting and Hasting

By the algorithm of SHA 256, the generation of hash by fixing the size of 256-bits will always be unique. The function is a one-way process; the result cannot be decrypted back to the original value. Before hashing, the password adds with the salt to obtain a unique safe hash password. Based on SHA-1 hashing, the salt password is generated, and the salt password will be unique and random. Using the hashing method of SHA-2, the hashed salt along with the password will be combined thus, with the same password as the user, and the combination will be provided with even and unique. This process will protect the password from the attack of brute force and the dictionary. When the attacker cracks one user's password, it will be hard for the attacker to crack all the passwords. Although a data breach is encountered based on the organization, it may be too difficult with the password when the password is broken. This password is compromised to consider with the full password. The entire user updates the password based on the notification sent immediately by the organization. It is unique for the hash for each salt, and the user now is hash with each rainbow table to measure the having based on the attacker who is hindered. A huge bottleneck will be created for the attacker. The entire process of secure password verification is shown in Pseudo code 4.3.

Pseudocode Password Verification

```
Begin
    Function passCheck
    userPass = password entered by the user
    hashPass = password from DB using user's key
    salt = salt from DB using user's key
    loc = location from user DB
    userHash = genPass ( loc, salt, userPass )
    If userHash equal to hashPass
      Then permit user into the application
    End If
    Else show message saying Password wrong
    exit the application
    End Function
End
```

4.4 Firebase Real-time Database

The end-user security application's medical data is stored in a Firebase Real-Time Database, developed using a distributed and collaborative data-management strategy. The application's client code can communicate securely with the database. User data is stored locally, and even when the app is not connected to the internet, real-time events will continue to trigger, creating a fluid and responsive experience for the user. When the client reconnects, the Real-time Database immediately reconciles any conflicts between the local modifications and the remote ones that happened while the client was offline. The necessary data can be stored in a tree format similar to JSON. You can see the database's skeleton in the diagram Fig.3.

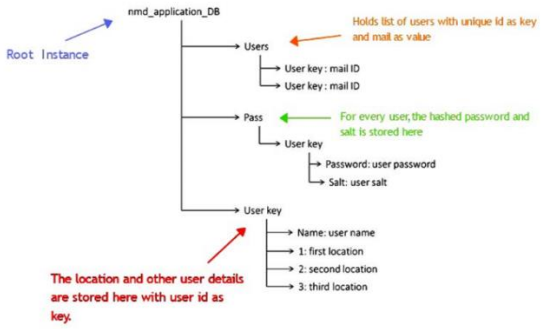

Fig.3 Proposed Firebase Database

5 Experimental Results and Discussions

This chapter demonstrates the result analysis with cost minimization of the authentication protocols in substantial computational cost and communication cost, as well as the security performance analysis of the suggested end-user authentication mechanisms and protocols against common threats. Each message sent and received throughout the registration and validation phases incur a communication cost according to the amount of data sent. Due to computational constraints, lightweight cyber security computation is insufficient for end-user authentication. Towards the result, it is common practice for protocol developers to strive to provide robust authentication methods. The amount of math utilized in the suggested protocols was cut down with the use of hashing, geo-location services, and random number generators. Table 1defines the notation used for the proposed protocols to measure the computational expense [27-36].

Table 1 Notation used for formal verification

Symbol	Meaning
U_i	i^{th} user
SR	Server
$username_i$	Unique identify of user U_i
PW_i	Strong user password
OTP	One Time Password
R_1,R_2,R_3	Secret random nonces
ΔT	Permissible time interval for the allowed delay

S_{key}	Shared session key
$AuthS_{Key}$	Calculated to authenticate session key
h(.)	Hash operation
||	Concatenation operation
⊕	XOR operation

5.1 Formal Verification using AVISPA

The tool Automated Validation of Internet Security Protocols and Applications (AVISPA) ("The AVISPA Project") "focuses on developing a button for the evaluation of a variety of Internet security-sensitive protocols and applications." These protocols are encoded in the High Level Protocol Specification Language (HLPSL). HLPSL is a powerful language used to model communication and security protocols. It consists of characterizations for each participant. "The role obtains its initial data from the parameters, which communicate with other roles via channels. These channels are presumed to be of the insecure Dolev-Yao threat model type, which allows an attacker to modify or delete the contents of transmitted messages.

The proposed method is called Multi-factor Authentication Schemes for Cloud-IoT Environment and is evaluated using the AVISPA tool's back-end CL-AtSe (Constraint Logic based Attack Searcher) and OFMC (On-the-fly Model-Checker) to produce output format (OF). The back-ends also attest to the scheme's security features, such as resistance to replay attacks, authentication, and key secrecy.Fig.3&4 depict the HLPSL language specifications of the user, session, goal, and environment roles in the proposed multifactor authentication strategy. All the key roles, such as those of the user and the system, are instanced with specific arguments in the session section. Intruder information is provided with the global constant and the make-up of one or more sessions found in the environment section. The AVISPA web tool provides details about the proposed scheme's simulation results, which is based on two commonly used back-ends, including OFMC and CL-AtSe. Fig.4shows that the proposed protocol is SAFE under two different back-ends, OFMC and CL-AtSe. Furthermore, the AVISPA simulation results show that the proposed scheme is secure against active and passive attacks.

```
role user (
SPi, RA, GWNODE, SD: agent,
H: hash_func,
S: symmetric_key
Snd, Rcv: channel(dy))
played_by SPi
def= local State: nat, IDi, PWi, BIOi, RPWi,A: text,
R, GWNi, Ci, Bi,Ai, TIDi, Rsdj, RUi, M3, Ti, M1, M2, T3, T4: text,
RPi, Rgwn, IDsdj, ID gwn, Kgwnsdj, Kgwnui, TIDinew, M11, M10, M12: text,
Gen, Rep: hash_func, T1, Sigmai: text
inite State:=0
transition
1. State = 0 /\ Rcv(start) =|>
%Registration phase
State':=1/\A':=new()/\R':=new()
/\secret({PWi,BIOi,S,A',R'},sr1,{SPi,RA})
/\Sigmai':=Gen(BIOi)/\RPWi':=xor(H(PWi.Sigmai'.A'),R') /\Snd({IDi.RPWi'}_S)
2.State=1/\Rcv({Ai'.TIDi'}_S)=|>
State':=2 /\ secret({PWi,GWNi,S,A',R'},sr2,{SPi,RA})
/\ Bi' := xor(H(IDi.Sigmai),A') /\ RPwi' := H(PWi.Sigmai,A')
/\ Ci' :=xor(H(IDi.GWNi),RPWi') /\ RUi' := new() /\ Ti' := new()
/\ M1' := H(IDi, GWNi') /\ M2' := xor(M1',RUUi')
/\ M3' := H(M2'.T1'.IDi.TIDi',RUi') /\ Snd({TIDi'.M2'.M3'.Ti'}_S)
/\ witness(RPi,GWNi,ui_gwn_t1,Ti')/\witness(RPi,GWNi,ui_gwn_rui,RUi')
3. State = 2 /\ Rcv({RUi'.Rgwn'.Rsdj'.IDi.IDsdj.IDgwn.
H(H(IDsdj.Kgwnsdj))}_H(IDi.Kgwnui). xor(TIDinew', H(TIDi'.H(IDi.Kgwnui).T3'.T4')).
H(H(H(IDi.IDsdj.IDgwn.RUi'.Rgwn'.Rsdj'.
H(H(IDi.Kgwnui)).H(H(IDsdj.Kgwnsdj))).T3').T4'.RUi').T3'.T4')=|>
%Ui's acceptance of T4 and TIDinew generated for Ui by GWN
State' := 3
/\request(GWNi,RUi,gwn_ui_t4,T4')/\request(GWNi,RUi,gwn_ui_tidinew,TIDinew')
end role
```

Fig.4 Role specification for the user of the multifactor authentication scheme in HLPSL

Simulation of the result shown in Fig.5 and it depicts clear performance of OFMC and CL-AtSe. In OFMC determined the protocol is SAFE and visited 16 nodes. OFMC results statistics clearly shows computational time 124 ms. The CL-AtSe result well defined the protocol for authentication is very SAFE.

```
role session (SPi, RA, GWNODE, SD: agent, H:hsh_func, S:symmetric_key)
def=
local S1,R1,S2, R2, S3, R3, S4, R4: channel (dy)
composition
user(SPi, RA, GWNODE, SD, H, S, S1, R1)
/\ regAuthority(SPi, RA, GWNODE, SD, H, S, S2, R2)
/\ gatewayNode (SPi, RA, GWNODE, SD, S, H, S3, R3)
/\ smartdevice (SPi, RA, GWNODE, SD, S, H, S2, R2)
end role

role environment()
def=
const spi, ra, gwnode, sd: agent, h:hash_func, s:symmetric_key,
gen, rep:hash_func, ui_gwn_t1, ui_gwn_rui, gwn_sdj_t2, gwn_sdj_rgwn,
sdj_gwn_t3, sdj_gwn_rsdj, sr1, s2: protocol_id
intruder_knowledge ={t1, t2, t3, t4, h, gen, rep}
composition
session(spi, ra, gwnode, sd, h,s) /\ session(i, ra, gwnode, sd, h, s)
/\ session(spi, i, gwnode, sd, h, s) /\ session(i, ra, gwnode, sd, h, s)
/\ sesion(spi, ra, gwnode, i, h, s)
end role

goal
secrecy_of sr1, sr2
authentication_on ui_gwn_t1, ui_gwn_rui, gwn_sdj_t2
authentication_on gwn_sdj_rgwn, sdj_gwn_t3, sdj_gwn,rsdj
authentication_on gwn_ui_t4, gwn_ui_tidinew
end goal

environment()
```

Fig.5 Role specification for the session, goal and environment of the multifactor authentication scheme in HLPSL

The role specification session, goal and environmental of the multi-factor authentication have assigned as per the testing tool by HLPSL. Every unique session has been verified with its nature. The combined proposed results are shown in Fig.6.

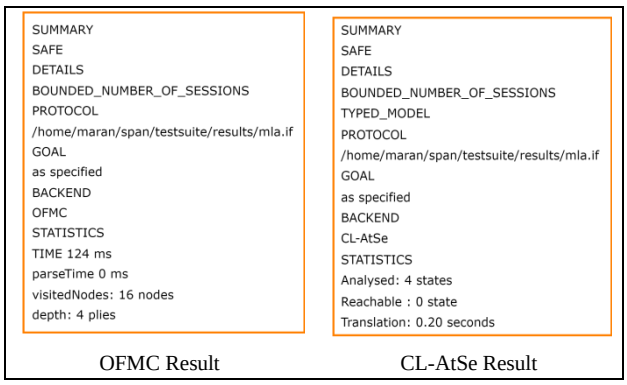

Fig. 6 Simulation result of the proposed multifactor authentication scheme for the OFMC and CL-AtSe back-end

5.2 Informal Verification using Security Parameter Analysis

In Table 4.2 compares the security features of the proposed scheme to those of the relevant scheme. This table shows that schemes are vulnerable to password-guessing attacks, suffer from user non-traceability attacks, do not support the user anonymity property and effective defense with phishing attack. Comparative analyses of the proposed scheme's performance are conducted with those of Khan, M.K. et al (2013), Siddiqui, Z et al (2014), Amin R et al (2015), Jiang, Q. et al (2016), and Ali R et al (2017). As can be seen in Table 4.2, each of these other schemes is vulnerable to a number of attacks, while the proposed scheme is completely secure. As a result, the strategy outperforms and out shields competing strategies. Many popular authentication methods lack complete security and are vulnerable to certain

security flaws. The proposed protocol, however, is immune to many common security flaws and has its own robust set of safeguards built right in the system.

5.3 Overall classification accuracy of the proposed model

A set of parameters is required to represent the effectiveness of a cyber-security system. Depending on the security system, the answer could be "Genuine access" or "Intruder Access." True or false are the only two choices here. Intruder Acceptance Ratio (IAR) and Genuine Acceptance Ratio (GAR) analyses are two examples of acceptance-based evaluations.Intruder Acceptance Ratio (IAR) analysis is the probability of an intruder being accepted as a genuine user. In this proposed multilayer authentication, the IAR is computed as the rate of the number of people falsely entered over the total number of users attempted. Genuine Acceptance Ratio (GAR) analysis is defined as the probability of the system's genuine users being accepted. In this proposed multilayer authentication, the GAR is computed as the rate of the number of legitimate users accepted by true attempts.

5.3.1Intruder Acceptance Ratio (IAR) Analysis

It is defined as the probability of an intruder being accepted as a genuine user. In this proposed multilayer authentication, the IAR is computed as the ratio of several people falsely accepted over the total number of users attempted. In Intruder Acceptance Ratio (IAR), the combined and proposed multilayer authentication system has been accepted with the minimal admission of users comparatively every single layer acceptance by this contribution. The proposed multi-layer authentication system allows the intruders with varied user scales of users from 1-10 to get 1.10%, and maximal admission of users 41-50 got 1.50%. It is shown in Fig.7, and Table 3illustrate the value obtained.

	SECURITY SCHEMES					
SECURITY PARAMETER	Khan, M.K. et al. (2013)	Siddiqui, Z et al. (2014)	Amin R et al. (2015)	Jiang, Q. et al. (2016)	Ali.R et al. (2017)	Proposed system
Defend Insider attack	Yes	Yes	No	Yes	No	Yes
Defend password guessing thread	Yes	No	Yes	Yes	Yes	Yes
Defend user anonymity attack	No	No	No	Yes	Yes	Yes
Defend impersonation attack	Yes	No	No	Yes	Yes	Yes
Defend temporary session key attack	No	NA	No	No	Yes	Yes
Defend replay attack	No	Yes	No	No	Yes	Yes
Defend phishing attack	No	No	No	No	No	Yes

Table 3 Comparison of IAR performance metrics- Single layer and Multilayer Authentication

Intruder Acceptance Ratio (IAR)

No of User	Single Layer			Proposed
	Layer 1 (Geo Location)	Layer 2 (E-mail OTP)	Layer 3 (Salting, Hashing)	Multi-Layer
1-10	3.70	2.40	3.20	1.10
11-20	3.80	2.40	3.25	1.15
21-30	4.00	2.45	3.30	1.30
31-40	4.20	2.45	3.50	1.45
41-50	4.50	2.50	3.60	1.50

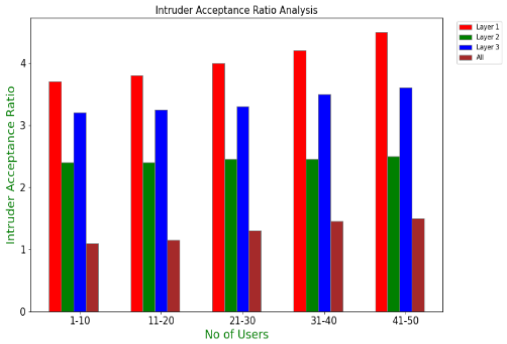

Fig. 7 Intruder Acceptance Ratio (IAR) Analysis

The proposed multi-layer authentication method has performed well in accuracy level to accept the false user to penetrate the security system. The proposed scheme was compared with various single layers involved in this verification method. We got a better restriction ratio to allow false users. Let us consider 41-50 users for IAR Analysis; layer-1 allows 4.50%, Layer-2 allows 2.50%, and Layer-3 allows 3.60%, but the proposed multi-layer authentication allows only 1.50% shown in figure 5.6.

5.3.2 Genuine Acceptance Ratio (GAR) analysis

In the Genuine Acceptance Ratio (GAR), GAR analysis has involved every layer of legitimate user acceptance. A user penetration has conducted several attempts to accept legitimate users with layer1, layer2, and layer3. The proposed multi-layer security analyzed in the minimal admission of users 1-10 got 98.90%, and maximal admission of users 41-50 got 98.50%. It is shown in Fig.8, and table 5.2 illustrate the value obtained**.**

Table 4 Comparison of GAR performance metrics- Single layer and Multilayer Authentication

Genuine Acceptance Ratio (GAR)

No of User	Single Layer			Proposed
	Layer 1 (Geo Location)	Layer 2 (E-mail OTP)	Layer 3 (Salting, Hashing)	Multi-Layer
1-10	96.30	97.60	96.80	98.90
11-20	96.20	97.60	96.75	98.85
21-30	96.00	97.55	96.70	98.70
31-40	95.80	97.55	96.50	98.60
41-50	95.50	97.50	96.40	98.50

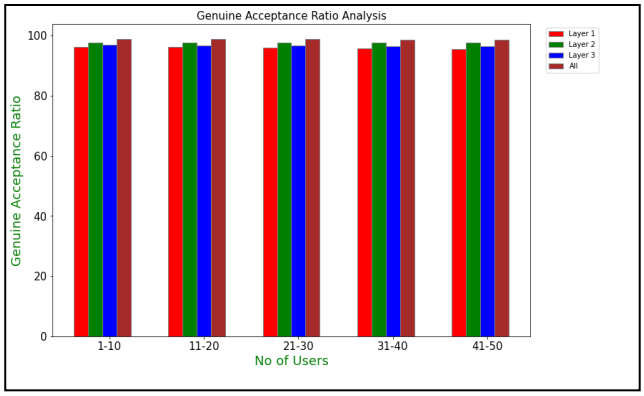

Fig. 8 Genuine Acceptance Ratio (GAR) Analysis

The proposed multi-layer authentication method has performed well in accuracy to allow the legitimate user to penetrate the user authentication security system. The proposed scheme was compared with various individual layers involved in this verification method. We got a better ratio to allow legitimate users. Let us consider 41-50 users for GAR Analysis. Layer-1 allows 95.50%, Layer-2 allows 97.50%, and Layer-3 allows 96.40%, but meanwhile, the proposed multi-layer authentication allows 98.50% shown in figure 5.7.

6 Conclusion

In this study, we developed a secure multi-factor authentication scheme that makes use of location verification, mail OTP verification, and salt and hash password verification. The proposed protocol was simulated using the AVISPA tool, and the simulation results show that it can withstand passive and active attacks as well as insider, password guessing thread, user anonymity, impersonation, temporary session key, replay, and phishing attacks. The informal security verification confirms that the proposed scheme is capable of defending against various types of security attacks. When it comes to attack resistance, the proposed protocol outperforms the relevant existing schemes.

Conflict of interest

The authors declare that they have no conflict of interest.

Ethical approval

This article does not contain any studies with human participants or animals.

Data Availability Statement:

The dataset analyzed during the current study is available in the zenodo repository, https://zenodo.org/record/8138182

References

[1] Khan, M.K., Kumari, S.: An Authentication Scheme for Secure Access to Healthcare Services. Journal of Medical Systems. 37(4), 9954-9954 (2013). https://doi.org/10.1007/s10916-013-9954-3.

[2] Mishra, D., Srinivas, J., Mukhopadhyay, S.: A Secure and Efficient Chaotic Map-Based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems. Journal of Medical Systems. 38 (10), 120-120 (2014). https://doi.org/10.1007/s10916-014-0120-3.

[3] Seifert, D., Reza, H.: A Security Analysis of Cyber-Physical Systems Architecture for Healthcare. Computers. 5(4), 27-27 (2016). https://doi.org/10.3390/computers5040027

[4] Cheddad, A, Condell, J, Curran, K., McKevitt, P.: A hash-based image encryption algorithm. Optics Communications. 283(6), 879-893 (2010).

[5] Ogini, N., Ogwara, N.: Securing Database passwords using a combination of hashing and salting techniques. IPASJ International Journal of Computer Science (IIJCS). 2(8), 52-58 (2014).

[6] Sriramya, P., Karthika, R.A.: Providing password security by salted password hashing using bcrypt algorithm. ARPN journal of engineering and applied sciences. 10(13). 5551-5556 (2015).

[7] Lakshmanan, T., Muthusamy, M.: A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes. 9 (2012).

[8] Amin, R., Biswas, G.P.: Remote Access Control Mechanism Using Rabin Public Key Cryptosystem. 525-533(2015).

[9] Bao, L.: Location Authentication Methods for Wireless Network Access Control. IEEE International Performance, Computing and Communications Conference. 160-167 (2008).

[10] Manoharan, S.: On GPS Tracking of Mobile Devices. In 2009 Fifth International Conference on Networking and Services. 415-418 (2009).

[11] Michael, K, McNamee, A., Michael, M.G.: The Emerging Ethics of Humancentric GPS Tracking and Monitoring. In 2006 International Conference on Mobile Business. 34-34 (2006).

[12] Mohamad, O.A., Hameed, R.T., Tapus, N.: Design and implementation of real time tracking system based on Arduino Intel Galileo', in 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). 1-6 (2016).

[13] Roxin, A., Gaber, J., Wack, M., Nait-Sidi-Moh, A.: Survey of Wireless Geolocation Techniques. In 2007 IEEE Globecom Workshops. pp. 1-9 (2007).

[14] Roxin, A., Gaber, J., Wack, M., Nait-Sidi-Moh, A.: Survey of Wireless Geolocation Techniques. In 2007 IEEE Globecom Workshops. 1-9 (2007).

[15] Mulla, A., Baviskar, J., Baviskar, A., Bhovad, A.: GPS assisted Standard Positioning Service for navigation and tracking: Review & implementation. In 2015 International Conference on Pervasive Computing (ICPC). 1-6 (2015).

[16] Michael, K., McNamee, A., Michael, M.G.: The Emerging Ethics of Humancentric GPS Tracking and Monitoring. In 2006 International Conference on Mobile Business. 34-34 (2006)

[17] Siddiqui, Z., Abdullah, A.H., Khan, M.K., Alghamdi, A.S.: Smart Environment as a Service: Three Factor Cloud Based User Authentication for Telecare Medical Information System. Journal of Medical Systems. 38(1). 9997-9997 (2014). https://doi.org/10.1007/s10916-013-9997-5

[18] Ali, R., Pal, A.K.: Three-Factor-Based Confidentiality-Preserving Remote User Authentication Scheme in Multi-server Environment. Arabian Journal for Science and Engineering. 42(8), 3655-3672 (2017). D.O.I. 10.1007/s13369-017-2665-

1
[19] Jiang, Q., Khan, M.K., Lu, X., Ma, J., He, D.: A privacy preserving three-factor authentication protocol for e-Health clouds. The Journal of Supercomputing. 72(10), 3826-3849 (2016). https://doi.org/10.1007/s11227-015-1610-x
[20] Limbasiya, T., Soni, M., Mishra, S.K.: Advanced formal authentication protocol using smart cards for network applicants. Computers & Electrical Engineering. 66, 50-63 (2018). https://doi.org/10.1016/j.compeleceng.2017.12.045
[21] Singh, A., Chatterjee, K.: A secure multi-tier authentication scheme in cloud computing environment. In 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]. 1-7 (2015).
[22] Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In 2016 10th International Conference on Intelligent Systems and Control (ISCO). 1-5 (2016).
[23] Wang, M., Abbass, H.A., Hu, J.: Continuous authentication using EEG and face images for trusted autonomous systems. In 2016 14th Annual Conference on Privacy, Security and Trust (PST). 368-375 (2016).
[24] Vegh, L.: Cyber-physical systems security through multi-factor authentication and data analytics. In 2018 IEEE International Conference on Industrial Technology (ICIT). 1369-1374 (2018).
[25] Maninder, S., Sarbjeet, S.: Design and Implementation of Multi-tier Authentication Scheme in Cloud. International Journal of Computer Science. 9(5), 1694-0814 (2012).
[26] Maninder, S., Sarbjeet, S.: Design and Implementation of Multi-tier Authentication Scheme in Cloud. International Journal of Computer Science. 9(5), 1694-0814 (2012).
[27] Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., Jin, Y.: Cyber-physical systems: A security perspective. In 2015 20th IEEE European Test Symposium (ETS), pp. 1-8 (2015).
[28] Lallie, HS, Shepherd, L.A.: Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security. 105, 102248-102248 (2021). https://doi.org/10.1016/j.cose.2021.102248
[29] Lim, S.Y., Kiah, M.M., Ang, T.F.: Security Issues and Future Challenges of Cloud Service Authentication. ActaPolytechnicaHungarica. 14(2) (2017 https://doi.org/10.12700/aph.14.2.2017.2.4
[30] Moller, D.P.F., Vakilzadian, H.: Cyber-physical systems in smart transportation.In 2016 IEEE International Conference on Electro Information Technology (EIT). 0776-0781 (2016).
[31] Rathore, H., Mohamed, A., Guizani, M.: A Survey of Blockchain Enabled Cyber-Physical Systems. Sensors. 20(1), 282-282 (2020). https://doi.org/10.3390/s20010282
[32] Sengan, S.V. S., Nair, S.K., V.I. J. M., Ravi, L.: Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future Generation Computer Systems. 112, 724-737 (2020). https://doi.org/10.1016/j.future.2020.06.028
[33] Vegh, L.: Cyber-physical systems security through multi-factor authentication and data analytics. In 2018 IEEE International Conference on Industrial Technology (ICIT). 1369-1374 (2018).
[34] Moller, D.P.F., Vakilzadian, H.: Cyber-physical systems in smart transportation. In 2016 IEEE International Conference on Electro Information Technology (EIT). 0776-0781 (2016).
[35] Ragaventhiran J., Vigneshwaran P., Prabu Ramadoss, Prisma Megantoro: An Unsupervised Malware Detection System for Windows Based System Call Sequences. Malaysian Journal of Computer Science, Special Issue on Computing, Communication and Cyber Physical Systems. 79-92 (2022). https://doi.org/10.22452/mjcs. sp2022no2.7
[36] Mishra, A., Pandi, V.: Intrusion Detection Using Feed-Forward Neural Network. In: So-In, C., Londhe, N.D., Bhatt, N., Kitsing, M. (eds) Information Systems for Intelligent Systems .Smart Innovation, Systems and Technologies. 324 (2023). Springer, Singapore. https://doi.org/10.1007/978-981-19-7447-2_9.