NOVEL APPROACH FOR END USER SECURITY ACCESS IN CYBER PHYSICAL SYSTEM USING MULTILAYER AUTHENTICATION

M.Maranco

Department of Computer Science and Engineering,
Coimbatore Institute of Technology,
Coimbatore, India.
maranco.m.phd@gmail.com

Dr.V.Manikandan

Department of Electrical and Electronics Engineering,
Coimbatore Institute of Technology,
Coimbatore, India.
manikantan.cit@gmail.com

Abstract

The exponential growth of cyber-physical systems (CPS), new security challenges have emerged. In this manuscript, we propose and systematize existing research on CPS security under a unified framework. In particular, the heterogeneity of CPS components and the diversity of CPS systems have made it very difficult to study the problem with one generalized model. However, there lack a systematic study of CPS security issues. Still, data and network system security remains an issue as well. In today's scenario level of security validation strategies is constrained to password protection and biometric at the max. But this doesn't suffice the high tech intruders who hack the security frameworks. Hence, this proposal is a novel attempt to provide more immune validation methods based on secured location user authentication technique using Reputed Mobile Location (RML). This implementation involves multifactor sequential verification system starting with a password protection followed by user's Geo- location in turn followed by the pseudo-randomly created alphanumeric code that is used as the token by the user through Mobile Application. These three walls of protection together curtail the hacks at all possible levels. This proposed approach is being tested as a prototype where reliable results are found in terms of accuracy, performance and security requirements for today's online services.

***Keywords*: Reputed Mobile Location (RML); Secure Hash Algorithm (SHA); Global Positioning System (GPS); One Time Password (OTP).**

1. The Main Text

Authors In the world, there are two factor authentications are widely used, they are user ID and password. Additionally, to the existing two factor authentication scheme utilizing user ID, password, one-time password OTP, the mobile number and geo location is utilized to recognize the user [1]. The physical characteristics like fingerprint etc., are the biometrics systems. There are two different types of biometric systems are utilized. They are facial images as well as Electroencephalography (EEG) signals [18]. Information from individual methods is linked in the level of matching score. This is essential to use a high security level. It could be attained by utilizing biometrics [14]. The combination of these two creates a two-factor authentication system. The two-factor authentication is user ID and password with an OTP token. It includes transmitting a software-based token via Transport Layer Security (TLS) tunnel, which is utilized to generate online OTP generated on the server side and OTP generated from the shared value on the android mobile phone [8]. Authentication based on location is a specific process to prove users identity and authenticity of appearance by identifying its presence in a unique location. A special combination of objects is needed to perform location-based authentication.
Firstly, the person to be identified and recognized must present the identity of the applicant.
Secondly, the user must take at least an authentication factor of human that can be recognized in a unique placement.
Thirdly, this unique placement should have an occupant capable of determining the individual's coincidence.

Authentication based on location is a standard process for granting access to an area by locating an individual. Discrimination is suggested to recognize the entry or exit of a person, to prevent two persons from accessing only one webpage [12]. The Global Positioning System (GPS), which helps guide and monitor applications, helps determine the exact location of objects on Earth. To implement the tracking function effectively, GPS depends upon numerous parameters like RF communication connection reliability, satellite geometry, GPS antenna location, NMEA (National Marine Electronics Association) design for GPS receiver, authentication based on location is a standard process for accessing a machine [11].

- Location-based authentication is an innovative process for providing additional information about the authenticity [11].

The authentication is indeed mandatory to access any secured system. Multilayered protection of sensitive data is a critical requirement to safeguard from anonymous users' attack. In present day context, the conventional username and password authentication is neither satisfactory nor competent against burning hacking issues. Thought it is widely used and simple to deny the user's access for a mismatch in the stored password using a remote authentication server, it has umpteen disadvantages. One noteworthy limitation of above mentioned one time authentication methodology is that there is instant and continual access to the protected resources right from the moment login is successfully initiated. This strategy may lead to security breach problems even in usual applications where security needed is less. So, needless to say its vital role in highly secured environments. Hence, need of the hour is to block the intruder's targets towards the post-authenticated session, otherwise known as the continuous monitoring or the continuous authentication. In such a technique, instead of recognizing certain unique times during the initial login stage or during a session, user verification repeats throughout the active session to monitor the user's presence and identity. The other regular threats are password capture, password guess, password crack, password replace etc.,

IDC study releases report on global smart phone exports, predicts that global smartphone exports will reach 1.86 billion units by 2019 in the next 5 years. As a result, ample number of ways is available to access services through smartphone. It could be mobile apps, widgets or even online browsers. Mobile apps are designed for a specific usage at any time once downloaded whereas browsers enable handheld website access. This great usage comes along with a huge number of threats as well. Although, cloud computing tries to solve various security and performance issues in the mobile environment, it is threatened by various types of cyber attacks such as malware, spyware, viruses because mobile appliances are strongly connected to the network and are widely used. A common example that could be seen today is the BYOD(Bring Your Own Device) concept in corporates where employees are encouraged to use their smart own device at work. In such cases, Mobile virtualization is proposed as a solution to prevent enterprise related secured data and other significant challenge posed by BYOD.

Hence in all the above mentioned circumstances, this proposal would be a gigantic leap over the existing levels of security. Hence password protection, verification and identification of user's location and pseudo randomly generated alphanumeric code are three mighty security standards that could provide high level security at all levels.

Pre-requisites

1. An Android device
2. Internet

2. Background

The mechanism design with implement in this study includes multifactor authentication where the factors are the multiple credential like user ID, password, pin and so on., and the other aspect is user smart phone and generated random dynamic randomized alphanumeric code secure sent to the user's appliance through mobile application. Before verify random code, middle factor verification is required namely, geo-location verification where the user verify themselves to the system by validating physical location latitude and longitude to the existing location database in cloud server. However, certain congruent models, mechanism is proposed and executed at the recent related works. The architecture and the work proposed in the manuscript provide certain new extensions and different innovative method [11,14,8].

2.1. *Usernames and Passwords*

The most traditional way of providing authentication to the legitimate users is through usernames and passwords. The username identifies which account does a client wants to access and the password proves the identity of the legitimate user. It is simplest method of authentication in which the encrypted and message digest of password is stored at the server side associated with the respective username which prevents it from any leakage of data or information about the original password of the account. It also referred to as single factor authentication.

Even this scheme of using usernames and passwords seems secure in sense but it still end up in being compromised. As the passwords being used by the users are very weak and they can be guessed very easily by applying a few list of combinations using the brute-force attack. Using the complex and longer passwords may be a possible solution to this problem and make it difficult for the attacker to guess a password through brute-force attack. But this idea of using longer passwords has its own disadvantages as they are difficult to memorize and the user have to store it somewhere else in his computer for use. This can also be a breach to security. Also the advances in the hardware make password more vulnerable and help to the attackers to be one step forward from the clients[4].

2.2. *SMS OTP and Geo-Locations*

One of the recent research works [12] proved that the two factor authentication scheme has great significance after introducing mobile banking. The schemes of two factor authentication were verify in terms of users information. This authentication scheme utilized to mobile banking systems. It works depends upon username, password and OTP where the individual receives through via mobile phone. Although, the authentication method based on existing OTP is identified to be effectual, the issue with kind of authentication scheme is the device loss. To enhance authentication abilities, geo-location-based authentication was developed. Geo Location authenticates the user in terms of their location. Geo-location was a term utilized to infer a user's geographical location depending on obtainable information. Geo-Location could recognize users in terms of cookies, IP address, MAC address and so on. When users authenticating, IP address of the host system was separated from a pocket header and identifies the owner of the IP address. It works by viewing an IPaddress on the service of WHOIS, so retrieve the physical address of user's. The location of IP address the data involve information like countries, regions, cities, postal/zip code, latitude, longitude, time zone. Geo-location typically indicates the latitude and longitude of a specific area, enhances by identifying several parameters other than geographical information. Many parameters like domain name, link speed, ISP, proxy, and so on could be obtained depending upon the data used by the IP address to define the location of user's [12]. At the time of generation if the location identified was matched with the location, OTP was created. If one time password matches, then the homepage become displayed or an alert message becomes send. With regard to the new location, the user must select the security questions and related answers that the user has selected. This GeoMob system was confirmed by the addition of certain types of authentication, which aids to find the identity change of person's for two-factor authentication based on user ID, password, one time password [12].

3. System design and implementation

In this manuscript, the RML system architecture is congruent with multifactor authentication scheme [12] and TMZ structure [18]. Figure1 represents the architecture of RML system. The RML system is separated as three level security authentications as shown in Figure1. They are user zone, security level and Security gateway. Level 1 indicates username and password, Level 2 indicates Geo-Location, Level 3 indicates case sensitive and alphanumeric token. We propose a smart mobile application that is differ from ordinary mobile application and also the secure application is isolated moreover it is equipped with reliable platform to the RML system. The trend is towards stealthy malware, a greater number of identity-related fraud and the increasing use insiders as a source of sensitive information. Security providers recommend organizations relying on authenticating users of IT systems to build comprehensive, multi-layer fraud detection and authentication system. Added to this, geo location information, web access behavior analysis to detect automated sessions, and botnet identification systems can get rid of a lot of bad traffic through device identification, before they are even allowed access. Basically Multi-layer authentication levels are grouped by any kind of security manner as discussed earlier. Following factors involved to enhance our security systems.

The conspicuous benefits of Multi Factor Authentication (MFA) are based on protection and account security, since its larger-scale adaptive at different secure-sensitive web utilizations. This manuscript proposes corresponding to design, execution, incorporation of multiple- layer, authentication system of multiple-factor to protect the webmail utilization. Comprehensive analysis of the executed system based on compliance to authenticate associated security policy of our centre is proposed.

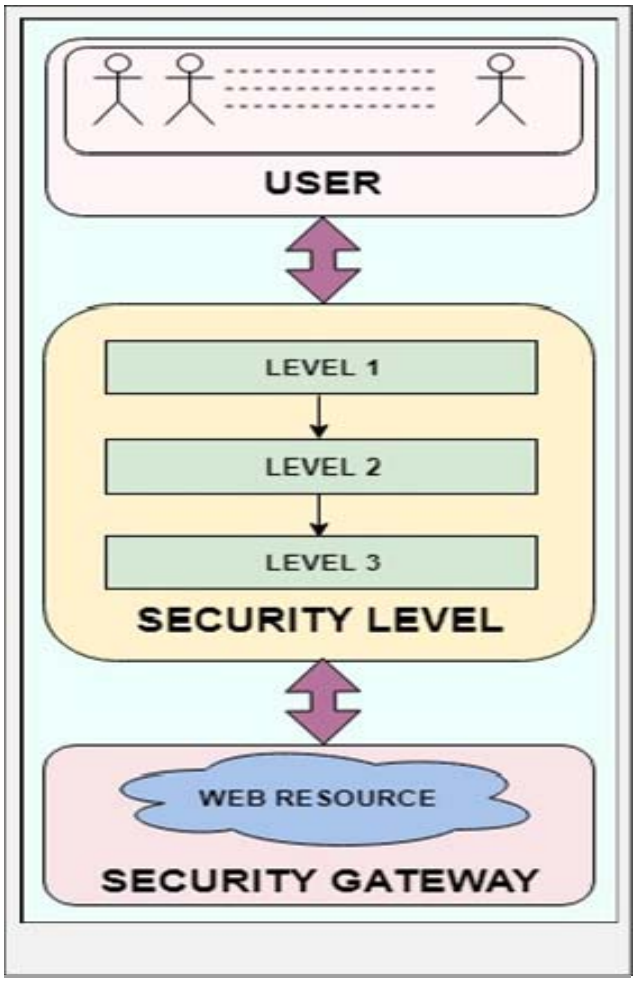

Fig.1 RML system architecture

3.1. *Password Verification (Layer – 1)*

A password refers to the letters or string utilized to the authentication of user to demonstrate identification or access approval to acquire access to resource that must be protect secret from unauthorized access.
SHA-3: A central required through NIST to SHA-3 hash function is sustaining the given output lengths:

- 224 bits
- 256 bits
- 384 bits
- 512 bits

3.1.1.Working:

Initially, input string is imposed along reversible padding rule and also cutting as r bits block. After that b bits level are initialized for zero then construction of sponge continues at 2 stages.

1. At absorption phase, r-bit input blocks signifies XOR ed in first state r bits, F is linked to the applications of the function. When entire input blocks are processed, the construction of sponge switches to compression stage.
2. In squeezing stage, primary state r bits are return as output blocks, F is linked with function application. Count of output blocks is optionally selected through user.

The construction of sponge utilizes state bits r + c that r upgraded by message bits among every Keccak-f application during absorption stage and output during squeezing stage. Rest of c bits is not straightly pretentious by message bits and is not output.
This function has nr rounds. Every round consists of input that has b = r +c bits.
Number of rounds based upon parameter1 : **nr = 12+2l**
SHA-3 are nr = 24 rounds as l = 6
It consists of various parameters that you may configure the input and output sizes and Keccak security level. The equivalent parameter is:

- b specifies state width, like b = r+c . b at change based on exponent l and may carry below values: b = 25 * 2 l , l =0,1,...,6
- This means the state may consist of width b ∈{25, 50, 100, 200, 400, 800, and 1600}. Observe the two lower parameters b = 25 and b = 50 are just toy values to analyze the algorithm also might not be utilized in perform.
- r is known as bit rate. r is similar with one message block xi length
- c is known as capacity. It should deal r+c is the width of valid state

i.e., r +c = b∈ {25, 50, 100, 200, 400, 800, 1600} The pseudo-code is determined below and Figure 2 shows SHA-3 Working Diagram, here, S indicates the state of lanes array. In padded message P is mentioned into array of blocks Pi, formulated into lanes arrays.

3.1.2.Pseudo code for SHA-3 Password verification:

The || operator indicates normal byte string concatenation.
Keccak[r,c](M) {
Initialization and Padding S[x, y] =0,
forall (x, y) in (0…4, 0…4)
P = M || 0x01 || 0x00 || … || 0x00
P = P xor (0x00 || … || 0x00 || 0x80)
Absorbing Phase
Forall block Pi in P
S[x, y] = S[x, y] xor Pi[x+5*y], forall (x, y) such that x+5*y < r/w S = Keccak-f[r+c](S)
Squeezing Phase
Z = empty string
while output is requested Z = Z || S[x, y],
forall (x, y) such that x+5*y < r/w S = Keccak-f[r+c](S) Return Z }
//keccak function
Keccak-f[b] (A) { forall i in 0…nr-1 A = Round[b]
(A, RC[i]) return A
}
//Round function
Round[b] (A, RC) {
θ step
C[x] = A[x, 0] xor A[x, 1] xor A[x, 2] xor A[x, 3] xor A[x,4] , forall x in 0…4 D[x] = C[x-1] xor rot(C[x+1], 1), forall x in 0…4 A[x, y] = A[x, y] xor D[x], forall (x, y)
in (0…4, 0…4)
ρ and π steps
B[y, 2*x+3*y] = rot (A[x, y], r[x, y]), forall (x, y) in (0…4, 0…4)
χ step
A[x, y] = B[x, y] xor ((not B[x+1, y]) and B[x+2, y]), forall (x, y) in (0…4, 0…4)
ι step
A [0, 0] = A [0, 0] xor RC
return A}

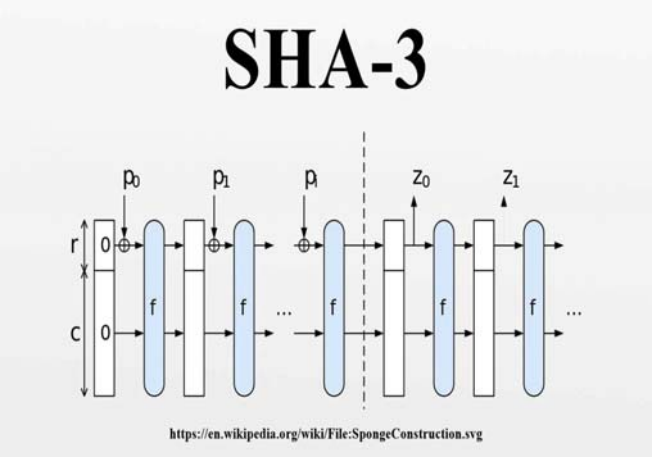

Fig. 2. SHA 3 Working Diagram

3.2. *Haversine Formula (Layer – 2)*

This formula determines the distance of a large circle among the two points in a sphere by its longitude as well as latitude. Significant at navigation is the unique case of the most common formula at spherical trigonometry, haversine law associate the spherical triangles sides with angles. The initial haversines table was introduced by James Andrew in 1805,[1] but Florian Cajori credits an earlier use by José de Mendoza y Ríos in 1801. The word "haversine" was introduced in 1835 by James Inman. Such names are derived from the fact, which is usually written based on the haversine operation, provided through haversin(θ) = $\sin^2(\theta/2)$. Figure 3 portrays the formulas can be written equivalent in many haversine basis, such as the older versine function (twice the haversine). Prior to the advent of computers, it was convenient enough to eliminate the division and multiplication by two factors for the inclusion of haversine table values including logarithms at the navigation, trigonometry texts of the 19th and 20th centuries. In those days, the haversine form is also convenient, with lack of coefficient before the $\sin^2$ operation.
Let Θ represents central angle amid either two points in a sphere:
Where,

- d implies distance between the two points (with large circle of the sphere; see spherical distance)
- r indicates radius of sphere.

The haversine formula hav of θ as following:

$$Hav(\theta) = hav(\varphi 2 - \varphi 1) + \cos(\varphi 1)\cos(\varphi 2)hav(\lambda 2 - \lambda 1) \quad (1)$$

To avoid using cosines which degrade in small angles

$$Hav(\theta) = hav(\varphi 2 - \varphi 1) + (1 - hav(\varphi 1 - \varphi 2) - hav(\varphi 1 + \varphi 2)\cos(\varphi 2).hav(\lambda 2 - \lambda 1) \quad (2)$$

Here,
• φ1 denotes point 1 latitude , whereas φ2 represents point 2 latitude
• λ1denotes point 1 longitude, whereas λ2 denotes point 2 longitude.
• Finally, the haversine function (half a versine) of an angle θ (used above mentioned differences in latitude and longitude) is:

$$hav(\theta) = \sin^2(\theta/2) = (1 - \cos(\theta/2)/2 \quad (3)$$

To calculate the distance d, apply the inverse haversine hav^{-1} to h=hav(θ)

$$d = rhav^{-1}(h) = 2r\sin^{-1}(\sqrt{h} \quad (4)$$

To substitute h=hav(θ) into (4)

$$d = 2r\sin^{-1}(\sqrt{hav(\theta)}) \quad (5)$$

To substitute (2) into (5)

$$d = 2r\sin^{-1}(\sqrt{hav(\varphi 2 - \varphi 1) + (1 - hav(\varphi 1 - \varphi 2) - hav(\varphi 1 + \varphi 2)\cos(\varphi 2).hav(\lambda 2 - \lambda 1))}) \quad (6)$$

Further improvement of (5), to apply (3) to (1) we get distance,

$$d = 2r\sin^{-1}\left(\sqrt{\sin^2\left(\frac{(\varphi 2 - \varphi 1)}{2}\right) + \cos(\varphi 1)\cos(\varphi 2)\sin^2\left(\frac{(\lambda 2 - \lambda 1)}{2}\right)}\right) \quad (7)$$

3.3. *Random Number Authentication (Layer – 3)*

Random Number Generator (RNG) is a device that creates an array of numbers or symbols, which does not predictable reasonably than a random possibility. RNG could be real hardware random-number generators (HRNG) that create real random numbers or pseudo-random number generators (PRNG).

OTP= a+b Mod Len
Where,
a – Random numbers using random ( )
b – External values
len – Length of the Alpha-numeric

4. System flow and algorithm

Cloud services are on increased usage even by commoners in the current era. Nowadays, the application user's especially social media and mobile App users themselves have access to update the data storage in cloud. Hence instant access to huge volume of data can be given access through W2 services which has brought in a great leap over the conservative W3 usage. In this proposal, the user is asked to register with username and password which is converted to JSON object and data is stored into a MYSQL table and further retrieved for faster access.

Second step is to setup a Primary Location namely PL that will be fixed by the App Admin and further 2 more secondary locations called SL1 and SL2 will be given by the user during registration. Further a radius of around 5 kms is set up in the App so that the user can access the app anywhere from PL or SL1 or SL2 or within 5 kms from any of these locations. A circumference of 5 kms is chosen around PL, SL1 and SL2 so that the user will be easily given a wireless or transmitter access to the app at ease within this area [12]. Once the user name, password identity and this Geo-Location tracking is done, the code generation by PRNG (Pseudo Random Number Generator) algorithm is followed [4]. Random numbers are given as input to the algorithm and a random alphanumeric code is generated. Figure 3 depicts the RML Implementation flow chart.
This will give a decent decrease in the time taken for encryption and decryption techniques that will be used in normal methodologies. Moreover, hacks can also be prevented in this way. This will be the final stage of authentication in the process succeeding which he user will be given full access to the application. The RML approach designed and implemented in multi-layer authentication, and the second layer of RML approach is embodied in reputation rather than the existing trust authentication shows in the following Pseudo code of RML approach implementation. The RML approach discriminates the three level of security authentication.

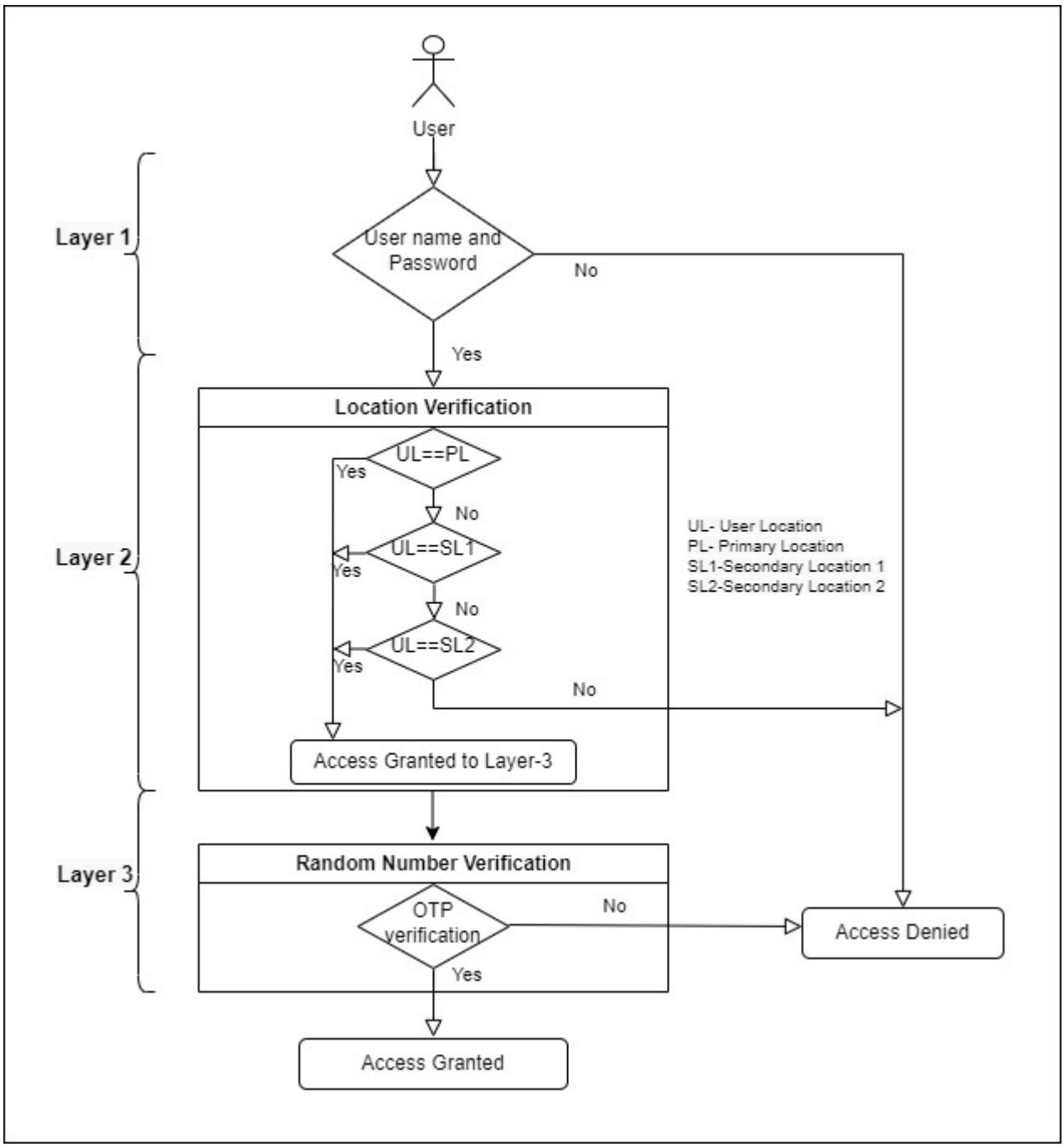

Fig.3. RML implementation Flow Chart

4.1. *Pseudo Code: System Flow*

```
Fix constant working Primary Location PL and Radius 'r'  by Admin:
Register username, password, Secondary Locations (SL1 and SL2) by user;
If (Resource Selection == mobile access || Resource Selection == web access)
    {
       If(Level 1 verification of username and
         Password)
           {
             if( current location == PL ||
                 current location == (PL+ r) ||
                 current location == SL1 ||
                 current location == (SL1+ r) ||
                 current location ==SL2||
                 current location == (SL2+ r) )
                  {
                    Generation of 3 minute Token Id
                     Copy Token Id and redirect to
                      Browser or
                      Login using User id, password
                      And Token Id (depending on
                      Web or mobile Access)
                        return True;
                  }
               else
                  {
                     return False;
                  }
            }
           else
                {
                   return False;
                }
       }
      else
            {
               return False;
            }
```

5. Result discussion

- Multi-layer authentication at the online environment denotes the ability to access multi-login name, password or different authentication devices or gain access to increasing sensitive information or high-risk transactions.
- This method can be utilized through raising extra security queries or by ask to additional passwords as more risky transactions are requested. Examples of multiple-layer authentication involve providing extra security.
- In a older technology they uses username, passwords as a main authentication ,To overcome that password based attacks we used a RML based verification as a main source as well as with multiple authentication factors such as Random Number Generation.
- The proposed approach for the end security using multi-level authentication efficiently works in various phases. In the first phase location-based authentication is used by getting the three preferred location from the user for the authorization.
- In the second phase our process is to validate the username and passwords are hashed using SHA-3. In the third phase verification is done on the locations preferred by the user and we are checking that the given locations are within the 5km radius using haversine formula.
- In the last phase we are generating tokens by integrating both latitude from the given location and pseudo random number generator algorithm with alpha-numeric six-digit code. Finally, the user can access our both web application and android app with enhanced security.

- The proposed approach has successfully measured and examined with various authentication type and we have achieved maximum accuracy of security system, which is shown in figure 4.
- The proposed system has verified with various security parameter with existing techniques of Khan M.K et al, Siddiqui.Z et al, Amin R et al, jiang Q et al and Ali R et al. Our proposed system has defended various effective authentication attacks comparatively with the existing approaches, it's shown in table 1.

Security Parameter	Techniques					
	Khan M.K et al	Siddiqui Z et al	Amin R et al	Jiang Q et al	Ali R et al	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.1. Result analysis table

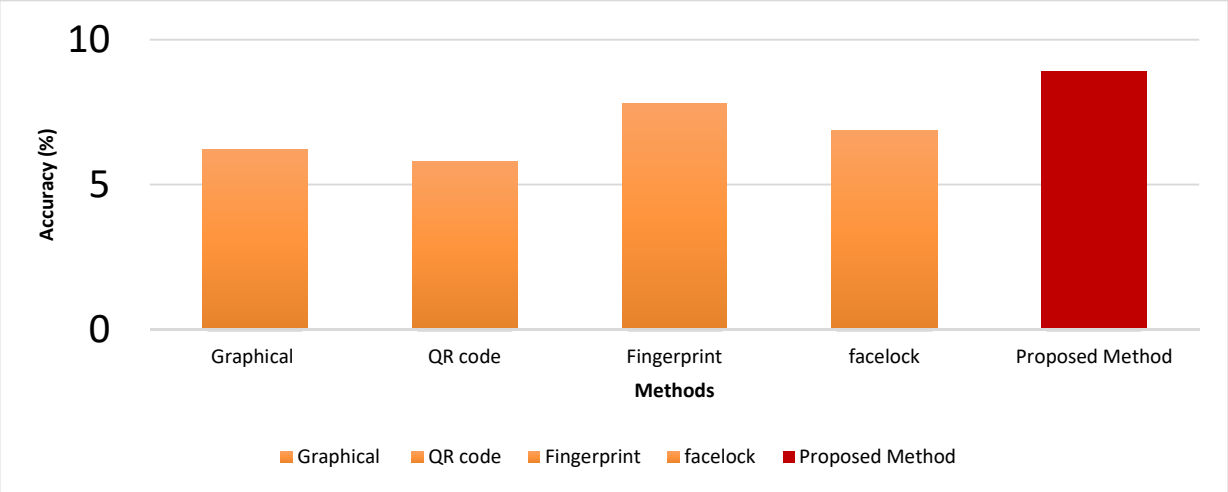

Fig.4. Accuracy of security system

6. Conclusion

Since the technology develops with more focus on the individual user, the authentication security has become more significant in the recent era. As many of the wearable devices along with the mobile devices would become a key feature of authentication, the proposed research work anticipated the time of processing when multiple methods were used in the three factor classes. This ensures greater authentication intelligence when compared to the existing methods of authentication owing to the inculcation of Multi-layer authentication at the online environment. This ensures and gain access to increasing sensitive information or high-risk transactions thus providing high end security for end users.

References

[1] Akoramurthy, B; Arthi, J (2017): GeoMoB — A geo location based browser for secured mobile banking. Eighth International Conference on Advanced Computing (ICoAC), pp. 83-88
[2] Ali, R.; Pal, A.K.(2017): Three-factor based confidentiality preserving remote user authentication scheme in multi-server environment.Arab. J. Sci. Eng. 42, 3655–3672.
[3] Amin, R; Biswas, G (2015): Remote access control mechanism using Rabin public key cryptosystem. Information Systems Design and Intelligent Applications, pp. 525–533. Springer, New York.
[4] Bandre, S. R (2015): Design and implementation of smartphone authentication system based on Color-Code. International Conference on Pervasive Computing (ICPC), pp. 1-5

[5] Danish, A; Sharma, L; Varshney, H; Khan, A.M (2016): Alignment based graphical password authentication system. 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 2950-2954.
[6] Eminagaoglu, M; Cini, E; Sert, G; Zor, D (2014): A Two-Factor Authentication System with QR Codes for Web and Mobile Applications. Fifth International Conference on Emerging Security Technologies, pp. 105-112
[7] Jiang, Q.; Khan, M.K.; Lu, X.;Ma, J.; He, D (2016): A privacy preserving three-factor authentication protocol for e-health clouds. J. Supercomput.72(10), 3826–3849.
[8] Kaur, N; Devgan, M; Bhushan, S (2016): Robust login authentication using time-based OTP through secure tunnel. 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 3222-3226.
[9] Kennao, Puleno; Mishra, Munish; Kesharwani, Lav (2016): Gps mobile banking: an advance security measures. International Journal of Development Research. 6. pp.7672-7674.
[10] Mulla, A; Baviskar, J; Baviskar, A; Bhovad,A (2015): GPS assisted Standard Positioning Service for navigation and tracking: Review & implementation. International Conference on Pervasive Computing (ICPC), pp. 1-6
[11] Patel, K; Han, H; Jain, A.K (2016): Secure Face Unlock: Spoof Detection on Smartphones in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2268-2283.
[12] Khan, M.K.; Kumari, S (2013): An authentication scheme for secure access to healthcare services. J. Med. Syst. 37(4), 9954.
[13] Mohamad O. A; Hameed, R. T; Tapus, N (2016): Design and implementation of real time tracking system based on Arduino Intel Galileo. 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1-6
[14] Wang, M; Abbass, H. A; Hu, J (2016): Continuous authentication using EEG and face images for trusted autonomous systems.14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 368-375
[15] Pilankar, P. S; Padiya, P (2016): Multi-phase mouse dynamics authentication system using behavioural biometrics. International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 1947-1950.
[16] Sayed, B; Traore, I; Woungang, I; Obaidat, M.S: Biometric Authentication Using Mouse Gesture Dynamics. IEEE Systems Journal, vol. 7, no. 2, pp. 262-274.
[17] Umar, S; Rafiq, Q (2012): A Novel Graphical Interface for User Authentication on Mobile Phones and Handheld Devices. International journal on advances in intelligent systems, 4, pp.380-387.
[18] Siddiqui, Z.; Abdullah, A.H.; Khan, M.K.; Alghamdi, A.S (2014): Smart environment as a service: three factor cloud based user authentication for telecare medical information system. J. Med. Syst. 38(1),9997

Authors Profile

M.Maranco, received M.E in Network Engineering from Anna University Chennai and currently pursuing Ph.D in Anna University Chennai. He is also working as an Assistant Professor in the Department of Computer Science Engineering (CSE) at Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India. His research interest includes cyber Security, Cyber Physical Systems, IoT and Cloud Security.

Dr.V.Manikandan, is working as Professor and Dean (planning) in in the department of Electrical and Electronics Engineering at Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India with more than 20 years of teaching and research experience. His Research interest includes cyber physical system, network analysis and synthesis, electric circuits and Optimization techniques.