Secured Authentication Method for Wireless Networks

Umesh Kumar[1], Sapna Gambhir[2]
[1, 2](Computer Engineering Department, YMCA University of Science and Technology, Faridabad, India)

ABSTRACT: *There are huge number of validation systems for system access focused around declaration, biometric, smart card with pin, password and so forth. One of the new and more prevalent validation procedures is OTP. The principle focal point of that is it is more secure as every time new secret key is utilized so recalling the password is no more needed. Each time new OTP is produced so no password is used over and over. If OTP generator is good then it makes this technique more secure. This paper describes EAP protocol and proposed EAP method for authentication.*

Keywords –*EAP, MD5, OTP, PEAP, SHA*

I. INTRODUCTION

As more administrations are getting to be online like net banking, online form filling and so on some of these services require authentication. Authentication is critical period of any correspondence. In the event that authentication technique is weak then 50% of fight is win by hacker however in the event that authentication strategy is solid then risk of getting hacked is less. Authentication [1] is the system to confirm the legitimacy of a client whether he/she is a legitimate client or not. When there is a talk regarding networking then clients need to fulfill some condition like having a valid user name and secret key of that server. In the event that user is valid then server permits him to get to the server's assets. So it is vital for a system to utilize such a robust strategy for verification so that no other than a valid client can get to the system rather not an individual who is not a legitimate client however utilizing hacking or whatever viable illicit path attempt to get to the system. When somebody tries to log on a workstation, they are generally initially asked for to identify themselves with a login name and password. Subsequently, this combination is checked against a current login-secret key legitimacy record to check if the mix is true. Provided that this is true, the client is verified. At last, a set of predefined consents and confinements for that specific login name is relegated to this client, which finishes the last step, approval. If information is not important then it might be accessed by anybody however in the event that it is classified then it rely on how the verification routines protects from unapproved access. So it ought to be strong to the point that it can't without much of a stretch be hacked and shouldn't be costlier than the data we are securing. Authentication can hold highly complex and secure strategy or be exceptionally straightforward. Straightforward type of verification is the transmission of share password between elements wishing to authenticate each other.

II. NEED OF AUTHENTICATION

Authentication is the methodology which permits the sender and recipient to approve one another. On the off chance that the sender and recipient of data can't appropriately validate one another, there is no trust in exercises or data given by other party. Let's understand this by the assistance of a sample: in a banking system, when somebody deposits cash in somebody banks account no confirmation is obliged in light of the fact that there is nobody who would store cash in other's record without any reason or it could be conceivable that by error he/she compose the wrong record number. In any case when the cash is withdrawn, then it requires validation and in verification it requires mark and pin number if cash is withdrawn by ATM [2]. So that nobody other than the authentic user can make any transaction without the consent. So validation is vital thing and it relies on upon the kind of data to be used.

III. METHODS OF AUTHENTICATION

There are different types of methods currently available for authentication. Currently there are many authentication methods available [1] .Some of the basic types are:

- Using Card & Pin

In this type of strategy a pin is given and card needs to be swiped and after that the pin is to be entered. Pin is only a mix of a few digits when considered the instance of ATM then the pin is four digit numeric qualities.

- Signature Verification [1]

This sort of confirmation is fundamentally in bank when withdraw cash by the assistance of the passbook. In this, sign on some form and different points of interest which is submitted. The approved individual matches the signature in your record and on the off chance that it matches the further transforming else solicitation to change to leave or reject your appeal. In any case now days set up of mark they likewise confirm the individual photographs so that any individual can't duplicate the mark and make utilization of it.

- Fingerprints [1]

Fingerprint is also one of the verification techniques to check the legitimacy of the client. The idea driving this is likelihood of two individuals having same unique finger impression is low.

- Hand Geometry

This innovation is formerly utilized as a part of Olympics was utilized to check the competitors. In this first client is asked to put his hand into a box this box consists of hand geometry reader which makes a bio metric layout of hand which is stored on microchip inside the users ID badge. This badge also holds the photographs of individuals. At the point when any client needs to get access to the system he was asked to put his hand into the reader. In the event that the result matched the value store in the badge, access permitted.

- Smart Card [2]

This type of concept use in MNC (Multi National Company) in which every member of company is assigned an ID card. So that when person enters the company he has to swap that card. If that card is legitimate then login possible otherwise not. But in some case cards are not swiped but they are just shown to verifier and now it is his job to verify the id of the employ of company.

- Username and Password [3]

This method is most widely used as a part of online login. In this method whenever a person access account online he/she needs to enter the username and password. Server first checks the legitimacy of username if it found correct then it checks the secret password of it. In the event detail matches server gives you access else shows invalid username or password.

- Voice Recognition [1]

Lots of research has been carried out to enhance automatic speech recognition. While most research was not done in light of security the result could be utilized to implement an authentication mechanism. In this a system record the voice of the client next time the client talk the same wording if these expression matches then client is legitimate else invalid . One crucial angle is that one must have the capacity to recognize an individual voice from a recording of it.

- Image Password [5]

In this we store password in the form of image. In this we have set of images first we select set of images in particular pattern. When next time we log in then we have to select the same images but also in the same pattern in which we store in the starting. If we it matches then it provides you the access else not. The main advantage is that remembering the numeric or alphabetic or both are not easy but remembering the images are easy. Also different type of attack like dictionary attack, brute force etc. not works in it.

- Retina

A person retina is unique and can help us to build very reliable authentication method. The problem with this method is people tend to display a natural fear about damaging their eyes and they are thus anxious that the device reading there retina might not be safe and also device used in this are very costly and only used in very high security military application.

- Face Recognition

It is used for facial recognitions. In this user face is used as password. This technology can commonly be seen in laptops for login. The new technique have to reduce the FAR and FRR considerably, even differentiating between someone holding the photo before the camera and an actual person sitting in front of the camera.

- Typing Speed

This is a biometric innovation focused around behavioral action. It is normally hidden from the end user as it is fused into a standard password and applies an additional test focused around the typing speed of the client to attain a more elevated amount of confirmation.

Protocols for Authentication

There are various security protocols which are currently available. Some of them are discussed below:

- MD5 [6]

Message digest (MD5) is focused around one way hash function. Fig.1. depicts its concept.

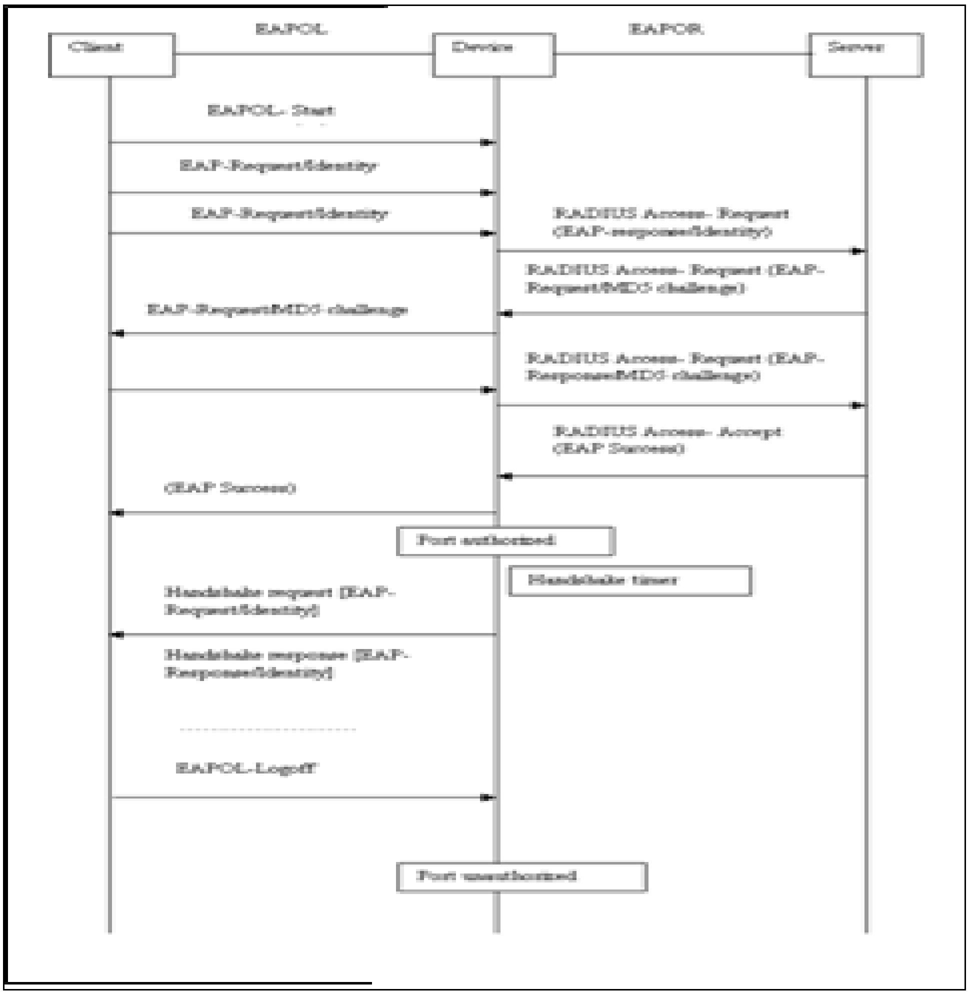
EAPOL
EAPOR
Client
Device
Server
EAPOL- Start
EAP-Request/Identity
EAP-Request/Identity
RADIUS Access- Request (EAP-response/Identity)
RADIUS Access- Request (EAP-Request/MD5 challenge)
EAP-Request/MD5 challenge
RADIUS Access- Request (EAP-Response/MD5 challenge)
RADIUS Access- Accept (EAP Success)
(EAP Success)
Port authorized
Handshake timer
Handshake request [EAP-Request/Identity]
Handshake response [EAP-Response/Identity]
EAPOL-Logoff
Port unauthorized

Fig. 1 EAP-MD5

It is an EAP well known method. In hash function a message of variable length is taken and a fixed length output we get called hash. It is an uneven validation strategy mean just the legitimacy of the client is checked however not the legitimacy of the server. In this the client password is not stored in plain text and also not sent through any medium in plain content. In MD5, methodology begin with registration stage in which client enters his username, secret key and other fundamental subtle details required by the server. At the point when client submits the data then hashing algorithm present at client side ascertains the hash of the password and sends to the server. Server stores the hash of the secret key to the corresponding username. At the point when client enters the password then hash of the password is sent to the server where server compares the stored hash value and the value it got. In the event that it matches then it shows welcome message else it shows wrong password or username blunder.

The primary preference of this convention is that it is easy to implement. Second, if some way or another somebody blocks the password or get that password he/she can't be decrypted on the grounds that producing the message having same hash capacity is extremely difficult. There were also a few disadvantages of this technique like there is no mutual authentication in this method so you are not certain that the server is valid or not. It doesn't infer a session key for its each session. It also suffers from different type of attack like reply attack, birthday attack, dictionary attack etc. It doesn't meet the vital prerequisite give in the RFC 4017 [7] so it should not be utilized for wireless communication.

- LEAP [4] [20]

LEAP (Lightweight Extensible Authentication Protocol) is developed by Cisco. It is based on challenge and response procedure. It also covers the two major weaknesses of WEP mutual authentication and session key which was missing in WEP. LEAP authentication starts with a pre shared secret key. First client sends a random challenge to server. The server decrypts the challenge and responds the challenge with encrypting it with session key. The client decrypts the challenge with session key if the value of challenge is same as it store at client then server is valid. Similarly server also verifies the client by similar method so by this mutual authentication is achieved. MSCHAP (Microsoft extension to challenge handshake Authentication protocol) protocol is also used in this method. As it overcome the drawback of WEP but it also suffers different type of attack like identity protection because whole message is sent in plain text. And also a hacker can easily sense the challenge-response pair transfer between client and server it also suffer a common dictionary attack etc.

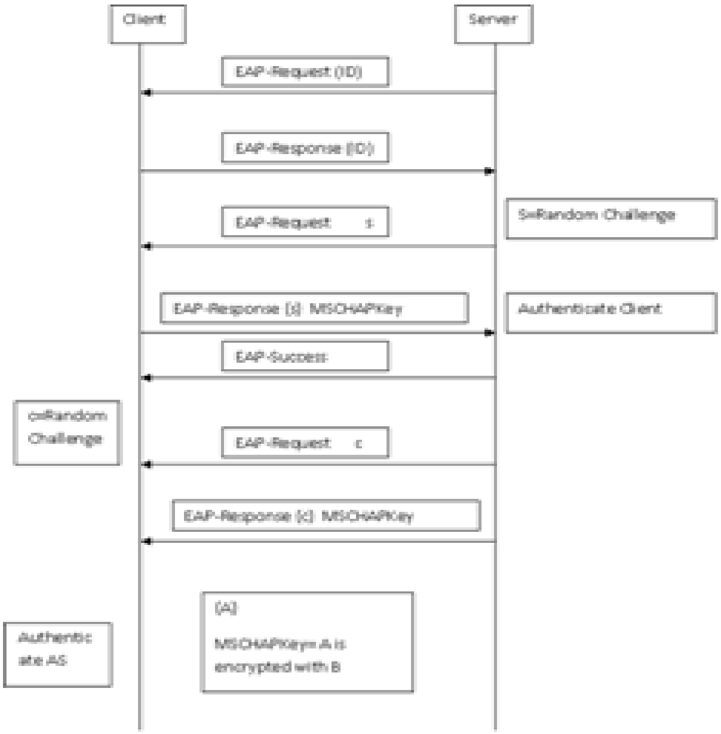

Fig. 2 EAP-LEAP

- EAP-TLS [9]

EAP-TLS is defined in RFC 2716. TLS (Transport Layer Security) is a standardized version of SSL (Secure Socket Layer). It is developed by Microsoft. It is a certification based Authentication methods for wireless LAN. It requests to install certificate on both client and server based on X.509 to provide dynamic session key distribution. First the client sends a random to server. Server in response of that sent its public key certification to client and request of client certification. As the client verifies the public key certificate it sent its certificate encrypted with server public key certificate to the server. As server receive client public key certificate it verifies that certificate to the issuing party. In this there is a third party who issues certificate to client and server. It is also possible that both are certified by different organization. Any organization who issues certificate charge some fixed amount after a fix interval to issues a certificate. As the certificate verification is done server sent a session key encrypted with client public key. As session key is also derived after that so that whole communication is encrypted by that session key. As we also keep in mind that message those encrypted by public key of user then it can be decrypted by only private key of the user not by any other key not even the public key by which we encrypt it. The main advantage of this is it resists most of the attacks like reply attack, MIMA (Man in the middle attack) etc. it support fast reconnect defined in RFC3748.

- EAP-TTLS [8]

EAP –TTLS is developed by Funk Company to solve TLS certificate problem (EAP-Tunneled TLS) it consist of two steps. In first step client authenticate the server by help of its certification and derived a session key. Secondly the client is authenticated in tunnel.

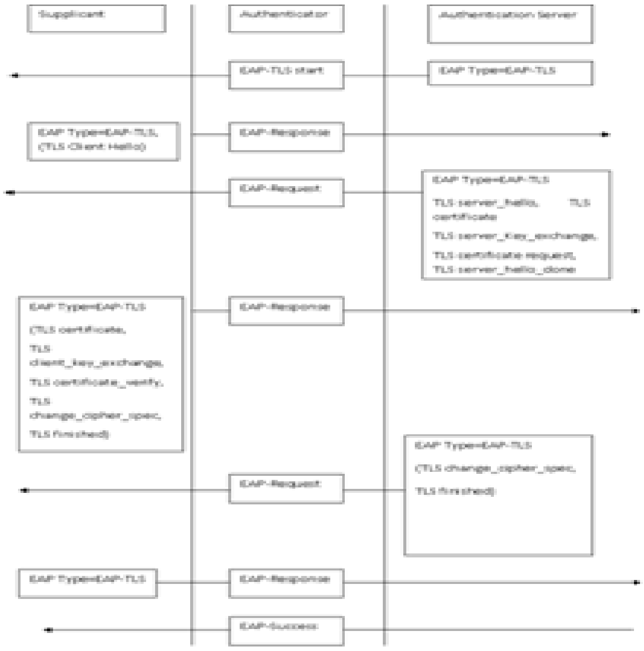

Fig. 3 EAP-TLS

Tunnel is created to keep the confidentiality of the information. EAP-TTLS provide high security during authentication it almost support almost all authentication protocol including legacy protocols and avoid the use of pre key infrastructure on client side due to this the overall cost of implementation also get decreases. The main aim of creating the tunnel is to protecting the authentication methods. So as it verifies the tunnel get collapses and it is client and server responsibility. By the help of tunnel the client identity is hidden so that hacker does not get any information of the communication and the user.

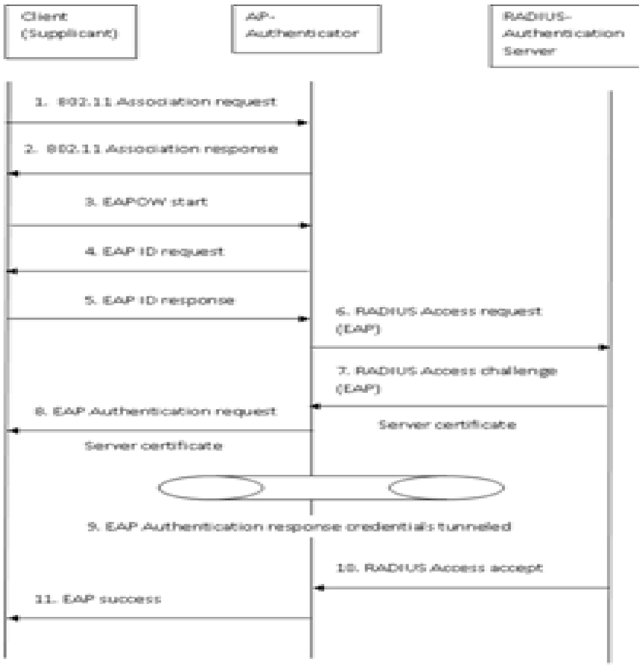
Client (Supplicant)
AP-Authenticator
RADIUS-Authentication Server
1. 802.11 Association request
2. 802.11 Association response
3. EAPOW start
4. EAP ID request
5. EAP ID response
6. RADIUS Access request (EAP)
7. RADIUS Access challenge (EAP)
8. EAP Authentication request
Server certificate
Server certificate
9. EAP Authentication response credentials tunneled
10. RADIUS Access accept
11. EAP success

Fig. 4 EAP-TTLS

IV. ARCHITECTURE OF EAP

Extensible Authentication protocol (EAP) [12] is not a protocol it is a frame work on the basis of which different protocols has been developed and new protocols can easily be added into it. It is mainly develop for WLAN (Wireless Local Area Network). We develop this protocol using EAP framework. E-EAP has three main components.

- E-EAP Client/Peer [13]

It is the user who wants to access the network services. It can be a computer or mobile devices. EAP Peer consist of three main component E-EAP which is our proposed protocol when we talk about general EAP then it consist of all set of EAP methods. E-EAP first it sent a hello frame which consist request to connect and also ask which protocol used for further communication but in our communication it used E-EAP. Second is EAP which we explain earlier and third is Supplicant mean client browser by help of which client can access network resources.

- E-EAP Authenticator [14]

It is the access point or NAS (Network Access Server). Which act as a broker between client and the Authentication Server. Initially it blocks the communication between client and server. Firstly it checks the validity of the user and then after it allows to access the network. The main task of it is to deliver the client request to server and also the server response to client. It's another task to display whether the authentication is successful or fail.

- E-EAP Authentication Server System [4] [7]

Server is called RADIUS [15] (Remote Authentication Dial in User Services). It store Information related to user account like login details, password etc. By the help of this information the server check whether the client existed in his data base or not. Similar to E-EAP peer side also have three main components. E-EAP method consist our proposed protocol E-EAP which consist OTP [16, 17] generator which generate OTP which used as password by user. And have mechanism system to deliver the OTP to client. It is also keep in mind that same method is used in by both for authentication second is EAP which we discuss earlier and last is RADIUS which is server itself.

- OTP Generation and Delivery Methods

This is the main portion of our protocol which make it different from other protocol there is similar type of protocol also existed but it is different from that so now move to our main part of the protocol.

- OTP Generator

To generate OTP [11] there are different type of ways or we can say methods are existed like Ping Pong [10], MD5 [6], SHA [10], Time and location Based [18] etc. But in our protocol we keep things simple but powerful. So we used SHA-1 for OTP generation. No the first thing comes in mind is what is SHA and how it works.

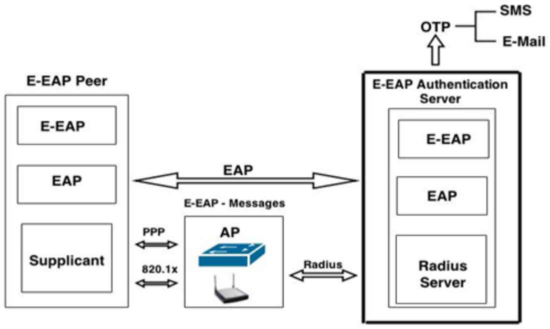

Fig. 5 E-EAP Architecture

- SHA-1 [10]

(Secure Hash Algorithm) is one of the most popular algorithm to generate hash of a message. It takes an arbitrary length data and converts into fixed length. When a message of any length < 2^64 bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then, be input to a signature algorithm which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature. Any change to the message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. We will show how SHA-1 works:

1. Initialize some variable
2. Pick up the String
3. Break the string into Character
4. Convert the character into ASCII codes
5. Convert number into binary
6. Add ‘1’ to the end
7. Append ‘0’s’ to the end until length of the message is congruent to 448 mod 512 and append original message length
8. Chunk the message into 512 bit chunk
9. Break the ‘Chunk’ into sixteen 32-bit words
10. Each chunk will be put through a little function that will create 80 words from the 16 current ones. And perform a left bit rotation by a factor of one. This is very simple. All you do is remove the first digit on the left and add a '0' to the end
11. Initialize variables
12. The main loop depending on what number word is being input, one of four functions will be run on it. And put them together.
13. The end.

- Delivery of OTP

As the OTP [11] is generated now our main task is to deliver to the client. It can be done via sending the same password through e-mail or SMS or both.

V. Problem Identification

Typical techniques for authentication are Password Based and there are two primary kinds of assaults, Dictionary attack and Brute Force attack. In the event that user select strong password then these attacks could be evaded. In any case we are bad in recalling solid password so we generally utilize powerless password which is not difficult to recall. What's more an alternate propensity is to utilize same password at distinctive area so there may be risk that if attacker by one means or another get your password then he can get to your private data of that record additionally diverse record. So we need to consider human element in our proposed authentication protocol. So one of the results is to OTP (One Time Password) [11] in this we don't need to recall anything aside from our record username which is our email id. Yet the disadvantage is OTP does not fulfill fundamental necessity [7] characterized in EAP. So we need to utilize some other alternate convention which can help us to give most extreme security. EAP-TLS [6] is a robust approach however the issues are:

- Client certificate [10]
- Cost
- Implementation

So our principle concern is to how to overcome on these issues. Cost and certification are connected to each other. Getting certificate from outsider is expensive thing on the grounds that it will charge some money to you after a fixed interval. Furthermore certificate trade and confirmation require some time. In the event that customer has no certificate then he can't tune in verification. On the off chance that some way or another we figure out how to discover an alternate route other than certificate which is comparably successful as certificate however less in expense can diminishes the overall cost. We can utilize OTP to check the legitimacy of the client which is simple and less excessive then TLS. At the same time the issues with this is getting this is simple by cloning of mobile SIM and email hacking also additionally hard to discover who get to that. Yet getting to two things at same time can take care of your issue in light of the fact that it provides for you more precise come about the user who utilized it. Second issue is human memory is restricted it can recall less things and on the off chance that it attempt to recollect new thing old things will overlook. On these issues problem can be solved by producing OTP each time when client login to the server.

VI. SECURED AUTHENTICATION METHOD FOR WIRELESS NETWORK

The proposed protocol E-EAP (Enhanced-Extensible Authentication Protocol) is based on the advantages of two protocols EAP-TLS and OTP. EAP-TLS is used for server certification and for session key. Session key is the key for a particular session with the help of that key we can encrypt the data which we are sending so that if someone somehow intercept our data then data will not be accessible. The concept of OTP is great because OTP (One Time Password) can be used only once. Due to which it can save us from different types of attacks like reuse attack, dictionary attacks etc. Our protocol starts with client request who want to communicate with server. As server receives the request it sends its certificate and asks for client ID. Client first verifies the server certificate and then sends its ID to server. Now server matches the client ID with the IDs which present at server Data Base. As it matches it generate an OTP corresponding to that ID. This generated OTP will be active for 1 hour and after that OTP will be deactivated. The generated OTP is first divided into two half and delivered to client via SMS and e-mail. First half will be sent via e-mail and second half will be sent via SMS. Now the user have to enter these two half into the space provided for password. If it matches with the OTP generated at server side then login is successful else failure message is delivered to client.

- Algorithm

1. Client wants to connect to the server so it sends hello message to server.

2. As the Server receive the hello message from client side. Server comes to know that client wants to communicate so it replies with hello message to client. Hello message of server contain its server certificate [10] which is issued by third party. By this the validity of the server can easily be checked. Whether it is valid server for which we are looking for or some other server which pretended to be valid server but it is not real.

3. Server request for client ID, by the help of client ID server want to check that whether the client is existed in its data base or not.

4. First client verifies the certificate of the server with the help of third party certificate client checks the validity of server. if third party verifies that certificate and confirm that it is issued by him then it's ok but if the third party reject that than there is no more communication between client and server because client get that the server is not valid server.

5. As third party verifies the certificate now the client is sure that the server is valid so client sent its ID to the server for further communication.

6. As Server receives the ID from client then it also tries to verify the client ID from its data base. If valid and present at server then further processing go else it shows error message.

7. If it found to be true then server try to find its e-mail id and mobile no. so that by using that it can send the OTP to client via SMS and E-mail.

8. Here password is divided into two half. As client receive the OTP via SMS [5] and E-mail. Now client receive OTP then he has to enter First half of password first then the second half of password in the password section. If the OTP doesn't match then it shows the error message.

9. Now server verifies that OTP is same that generated by him against the client ID or not.

10. If OTP is valid the message of success is shown else message of invalid OTP is display.

11. Now the client generate a Pre Master Secret key [19]

12. Now it time to share session key with server so the best way is to encrypt it with server public key and send it to server as we all know that information encrypted with server public key is only opened by private key which always present at server.

13. As server decrypt it with its private key and agree to use that session key for that particular session.

Now whole communication is encrypted with session key. It is one of the best ways to secure the information from third party to access. And also increases the reliability for the communication.

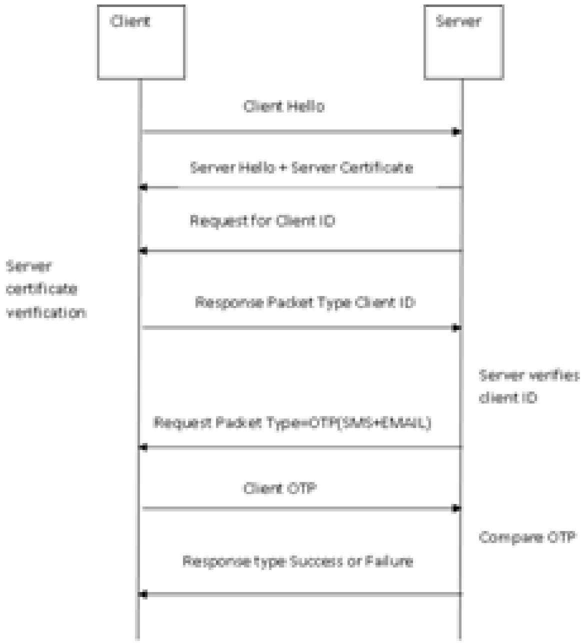
Client
Server
Client Hello
Server Hello + Server Certificate
Request for Client ID
Server certificate verification
Response Packet Type Client ID
Server verifies client ID
Request Packet Type=OTP(SMS+EMAIL)
Client OTP
Compare OTP
Response type Success or Failure

Fig. 6 E-EAP Algorithm

- Comparison

Table 1.1 presents a multi-aspect qualitative comparison between five different protocols and proposed protocol. Important aspects like the implementation, certification whether it is client or server, different type of attacks like dictionary, MITM (Man in The Middle), reply attack, cost and other security issues.

Table.1. Multi-Aspect qualitative comparison study

EAP-Type	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	EAP-PEAP	E-EAP
Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes
Deployment Difficulties	Easy	Easy	Hard	Moderate	Moderate	Easy
MITM Attack Protection	No	Yes	Yes	No	No	Yes
Dictionary Attack Protection	No	No	Yes	Yes	Yes	Yes
OTP Generator	No	No	No	No	No	Yes
Delivery of password by Mail and SMS	No	No	No	No	No	Yes
Low Cost	Yes	Yes	No	No	No	Yes
Require Remember Password	Yes	Yes	No	Yes	Yes	No
Reuse Attack Protection	No	No	-------	No	No	Yes

VII. CONCLUSION

The proposed approach discussed about the authentication, its security issues and its prevention technique. Authentication is a very important for offline and online user. It checks the validity of the user whether he/she is valid user or not. If authentication is not there than everyone can access others information either it is confidential or not. Its presence in system increases the security. Presently there are many protocols but they have their advantages and disadvantages. The proposed E-EAP method satisfies the requirement defined in RFC 4017. Other feature such as no reuse attack and cost is also including in our E-EAP method. In this protocol we used e-mail and SMS to deliver the password to client which increases lot of security in that. In addition, the passwords generator we used SHA-1which decrease the chance of guessing the password or cannot be driver by looking few set of passwords. We used different medium to send password to user. But people think that OTP concept is already implemented. We know that OTP is implemented but the drawback is that any user can easily access one thing like if complete password is sent via SMS then the attacker have only one thing to access your mobile to get the password. But in our protocol password is first divided in two half and these two halves of password is sent via e-mail and SMS. Both passwords are different and user has to combine them to login in the system. So this will give you chance to easily find out the attacker because there are very less no. of people who can access both of your things at the same time.

VIII. FUTURE WORK

In the future works, we will try to provide a formal security proof to prove that our E-EAP Method is truly secure. Although we have examine that our E-EAP method satisfies all security requirements, but we still consider that they are not enough. Besides, it is quite possible that in future SMS system also get hacked which has very less chance but we have to consider that also so we have to keep trying to find new way by which authentication can be made more secure. There may also little delay in receiving SMS time. It can be possible that there is lot of rush/load in the mobile network traffic. Which create little bit of delay in login. Also for login we have to access our mail every time so we have to find another way by which we can replace it with mail system. There are no other EAP methods provide formal security proof to prove that they are secured. Therefore, we will keep trying to find new way for more secure authentication mechanism.

REFERENCES

[1] Mark Vandenwauver, Rene Govaerts and Joos Vandewalle, Overview of Authentication Protocols, Katholieke University Leuven, Belgium.

[2] D S. Stienne, Nathan Clarke and Paul Reynolds, Strong Authentication for Web Services using Smartcards, 7th Australian Information Security Management Conference, 2013.

[3] B. Lloyd and W. Simpson, PPP Authentication Protocol, Internet Engineering Task Force (IETF) RFC 4017 October 1992.

[4] Khidir M. Ali and Ali Al-Khalifah, A Comparative Study of Authentication Methods For Wi-Fi Networks, 3rd International Conference on Computational Intelligence Communication System and Network, July 2011, 190-194.

[5] C. Shyamala Kumari and M. Deepa Rani, Hacking Resistance Protocol For Securing Passwords Using Personal Device, 7th International Conference on ISCO, Jan 2013, 458-463.

[6] Jyh-Chen and Yu-Ping Wang, Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience, IEEE Communications Magazine, Dec 2005, 26-32.

[7] D. Stanley, J. Waliker and B. Aaboba, EAP Methods Requirements for Wireless LANs, Internet Engineering Task Force (IETF) RFC 4017, March 2005.

[8] Bakytbek Eshmurzaev and Gokhan Dalkilic, Analysis of EAP-FAST Protocol, 34th International Conference on Information Technology Interfaces Cavtat, Croatia June 2012, 417-422.

[9] Anjali K. Rai, Shivendu Mishra and Vimal Kumar, Strong Password Based EAP-TLS Authentication Protocol for WiMAX, International Journal on Computer Science and Engineering, Vol. 02, No. 08, 2010, 2736-2741.

[10] Bahareh Shojaie, Iman Saberi , Mazleena Salleh, Improving EAP-TLS Performance Using Cryptographic Methods, International Conference on Computer & Information Science, June 2012, 760-764.

[11] Kenneth G. Paterson and Douglas Stebila, One-Time-Password-Authentication Key Exchange**,** ACISP, Berlin Heidelberg 2010, 264-281.

[12] Kwang-Hyun Baek, Sean W. Smith, David Kotz, A Survey of WP A and 802.11i RSN Authentication Protocols, Dartmouth College Computer Science Technical Report TR2004-524 November 2004.

[13] Weili Huang and Renle Li, WLAN Authentication System based on the Improved EAP-TLS Protocol, Web Mining and Web based Application, Pacific-Asia Conference, 2009.

[14] Samuel Sotillo, Extensible Authentication Protocol (EAP) Security Issues, East Carolina University, 2007.

[15] C. Rigney, et al., Remote Authentication Dial In User Services (RADIUS), IETF, RFC 2865 June 2000.

[16] D. M'Raihi, S. Machani, M. Pei and J. Rydell, TOTP: Time-Based One-Time Password Algorithm, Internet Engineering Task Force (IETF) RFC: 6238 ISSN: 2070-1721, May 2011.

[17] J. Linn and M. Nystroem, OTP Methods for TLS, Networking Working Group Dec 2006.

[18] Wen-Bin Hsieh and Jenq-Shiou Leu, Design of a Time and Location Based One-Time Password Authentication Scheme, 7th IWCMC, July 2011, 201-206.

[19] Myeonggil Choi, Nguyen Manh Thang, An Exensible Authentication Protocol with Transport Layer Security and One Time Password in Multi Hop Mesh Network, Recent Researches in Business Administration, Finance and Product Management ISSN: 978-960-474-265-3.

[20] Umesh Kumar, Parveen Kumar and Sapna Gambhir, Analysis and Literature Review of IEEE 802.1x Authentication Protocols, International Journal of Engineering and Advanced Technology, Vol. 03, No. 05, June 2014.