www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 01, January 2024, pp : 350-357

e-ISSN : 2583-1062

Impact Factor : 5.725

A REVIEW ON VARIOUS AUTHENTICATION TECHNIQUES AND PROTOCOLS

Md. Shahnawaz[1], Mr. Manoj Yadav[2], Mr. Sudeesh Chouhan[3]

[1]Research Scholar, Dept. of Computer Engineering, SOE, SSSUTMS, Sehore, India

[2]Assistant Professor, Dept. of Computer Engineering, SOE, SSSUTMS, Sehore, India

[3]Assistant Professor, Dept. of Computer Engineering, SOE, SSSUTMS, Sehore, India

ABSTRACT

Authentication is the process of verifying the authenticity of the client to determine its authenticity. If the user is trusted, the server allows access to its properties. There are many authentication methods and protocols to protect server assets from unauthorized access. This article provides an overview of the various factors, protocols, and methods involved in authentication and their importance in real-world scenarios. Extensible Authentication Protocol (EAP) is a framework that aims to provide flexible authentication for wireless networks. The purpose of this review is to explore the most widely used authentication methods and evaluate their strengths and weaknesses.

Keywords: Authentication, authentication protocols, factors, EAP, TLS, TTLS, MD5, LEAP, PEAP

1. INTRODUCTION

Today most of the services are going online, so a lot of personal information gets on the internet and it is important to keep them secured from hackers to avoid leaks. Every time we use an authentication system is used to get access to a service, identity is released in terms of username, passwords and biometric information, which can be abused by the service providers for tracking our behavior, profiling our usage of the service or even for impersonation. So, with the steep increase of the number of services are getting the online treatment, it is reasonable to expect a strengthening demand for secure and reliable authentication systems. Authentication is the methodology which permits the sender and recipient to approve one another. It can be done by providing a username and a password to identify themselves against a legitimate record in the database to check the combination is correct. In the event that user is valid then server permits him to get to the server's assets. So it is up to the authentication protocols defined to protect the server's assets from getting unauthorized access and they should not be costlier than the data which is being secured.

This paper is organized in the following manner. Section I starts with the need for authentication in systems for providing security. Section II contains the motivation behind the paper introducing the role of authentication protocols. Section III introduces the various factors of authentication Proceeding ahead, Section IV provides the overview of various commonly used authentication protocols. Section V introduced the details of some of the methods that can be used with the authentication protocols. Section VI describes the related work for authentication protocols. Finally, Section VII concludes the survey with future directions.

2. MOTIVATION

Security can be considered the backbone of any distributed system and is provided by authentication protocols, so it is necessary for these functions to work correctly. An authentication protocol is a type of computer communications protocol or cryptographic protocol that specially designed for transfer of authentication data between two entities. It is also the very important layer of protection that can be needed for secure communication in computer networks. The primary goal of an authentication protocol is to establish the identities of the parties who participate in the protocol. There can be a secondary goal to distribute secret session keys for further communication which is a key element in providing security in distributed networks both wired as well as wireless.

3. FACTORS OF AUTHENTICATION

Identification occurs when a client states its identity (such as with a login id), and authentication occurs when clients prove their identity. For example, clients are authenticated when they provide the combination of correct username and password. Permissions, rights, and privileges are then granted to authenticated clients. The following Figure 1. shows the three common factors of authentication [1]:

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 01, January 2024, pp : 350-357

e-ISSN : 2583-1062

Impact Factor : 5.725

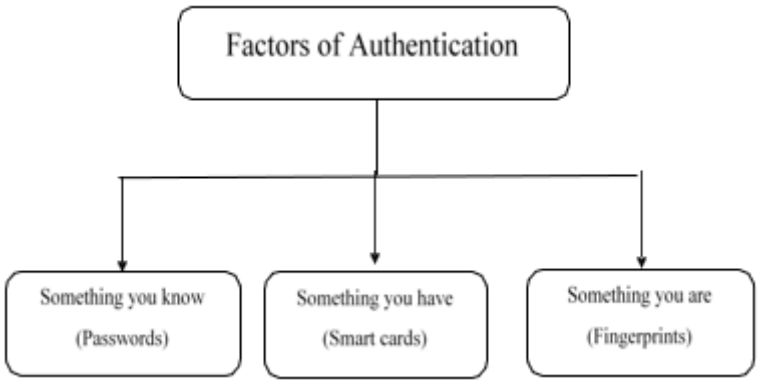

Figure 1. Factors of Authentication

- The "something you know" factor is the most used factor and generally involves a password or a personal identification number (PIN). In majority of the systems the passwords are encrypted instead of storing it as a plain text. This type of authentication does not require any hardware support and consume less processing power. This method has many drawbacks, some of which are:

1) Passwords are easy to guess.

2) Placing the password in a highly visible area.

3) Unsafe due to malpractice of eavesdropping.

- The "something you have" factor involves the items such as smart cards or tokens. A smart card is a small sized card having an embedded certificate used to identify the owner. The user inserts the card into a reader to authenticate the individual. A token is a small device having an LED display that displays a number and the number is synchronized with an authentication server. The user types in the number displayed in the token on a web page. If the number typed by user matches the number known by the server at that time, the user is authenticated.
- Biometric methods indicate the "something you are" factor of authentication. Biometrics are those which are identified by human attributes, such as fingerprint, voice print and iris scan. Biometric feature of a user is so unique that even twins cannot have the same biometrics. Moreover, these security mechanisms are costlier but are most reliable among all three factors of authentication. Many recent authentication protocols are using the combination of these factors to enhance the security.

4. TYPES OF AUTHENTICATION PROTOCOLS

4.1 Extensible Authentication Protocol (EAP)

EAP is an authentication protocol which is defined in RFC 3748. It is an authentication framework that is designed to run on the data link layer where IP connectivity is not available [2]. EAP was designed to work with Point-to-Point connections, and was subsequently adapted for IEEE 802 wired networks as well as wireless LAN networks and over the Internet. EAP architecture involves three main components. The involvement of these components can be illustrated in the protocol stack shown in the Figure 2. It provides a basic request/response protocol framework over which various EAP methods can be implemented. There are currently about 40 different methods defined. Some authentication methods are predefined like LEAP, TLS, POTP, MD5, PSK, TTLS an SIM.

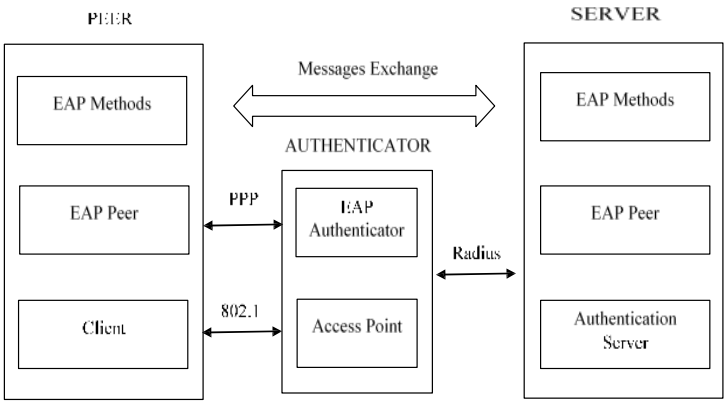

Figure 2. EAP Protocol Stack

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 01, January 2024, pp : 350-357

e-ISSN : 2583-1062

Impact Factor : 5.725

These methods support authentication credentials that include challenges, password, certificates and keys. Other methods can be added without changing the network protocol or defining new ones. The main advantage of the EAP architecture is its flexibility to adapt to various authentication methods. The Figure 3. shows the basic structure of the EAP message flow.

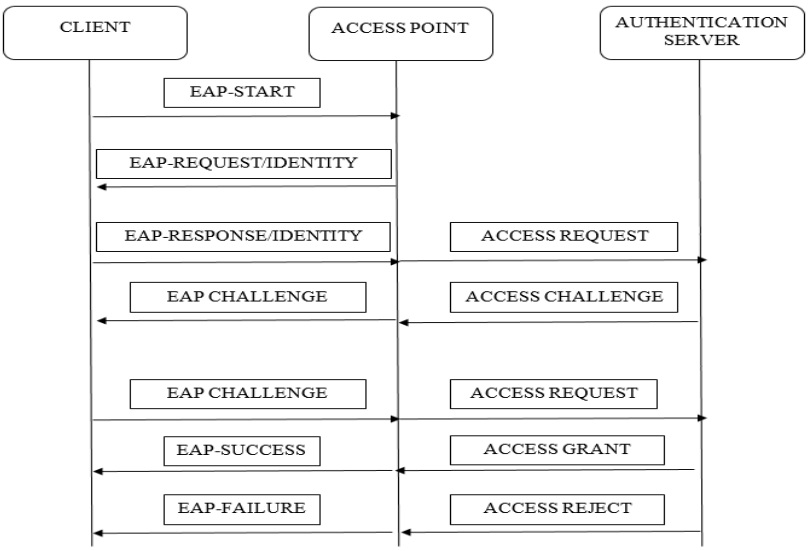

Figure 3. EAP Flow Diagram

4.2 Password Authentication Protocol (PAP)

It is a user authentication protocol that sends the credentials to the authentication server unencrypted as plain text. It is one of the oldest protocol for the verification of packet. It uses a two-way handshake process. The verification of the packet is started by user sending packets with credentials (username and password) at the starting of connection. The characteristic of sending credentials to the server in plain text gives a major risk of unauthorized access to a user who can capture the data packets using a protocol analyser to obtain the credentials. PAP is vulnerable to the attacks like Eavesdropping and Man-in-the-middle based attacks. Remote access control authentication can also be done using PAP. It has an added advantage of being compatible with many different server types running on different OS. The following Figure 4. gives the basic flow of PAP model

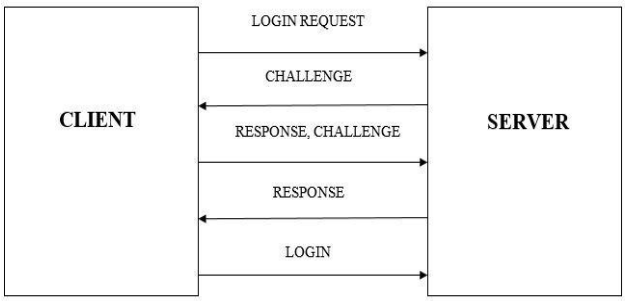

Figure 4. PAP Flow Diagram

4.3 Challenge Handshake Authentication Protocol (CHAP)

It uses a three-way handshake which is illustrated in the Figure 5. The authentication method depends on a "secret challenge" known only to the authenticator and that peer. Server can send a random string (usually 128B long). Client uses the string and password received as parameters for MD5 hashing and sends the result together with username in plain text. Server applies the hashing function using the same username and then compares the calculated and receive hash. If the result matches, then authentication is successful otherwise process takes you back to the login page. Playback attacks are prevented using this algorithm by the peer through the use of changing identifier and a variable challenge value.

4.4 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

It encrypts password information before transmitting it over a PPP link using the industry-standard MD5 one-way encryption method. There is no need of plaintext or reversibly encrypted passwords the way CHAP does. The protocol is available in two versions, MS-CHAPv1 (defined in RFC 2433) and MS-CHAPv2 (defined in RFC 2759). MS- CHAPv2 supports two-way authentication to verify the identity of both sides of a point to point connection and provides separate cryptographic keys for transmitted and received data based on the user‟s password and the arbitrary challenge string. It is more secure than

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 01, January 2024, pp : 350-357

e-ISSN : 2583-1062

Impact Factor : 5.725

version 1 because the same user will have separate keys generated for each session. It piggybacks a peer challenge on response and authenticator response on success packet to achieve mutual authentication.

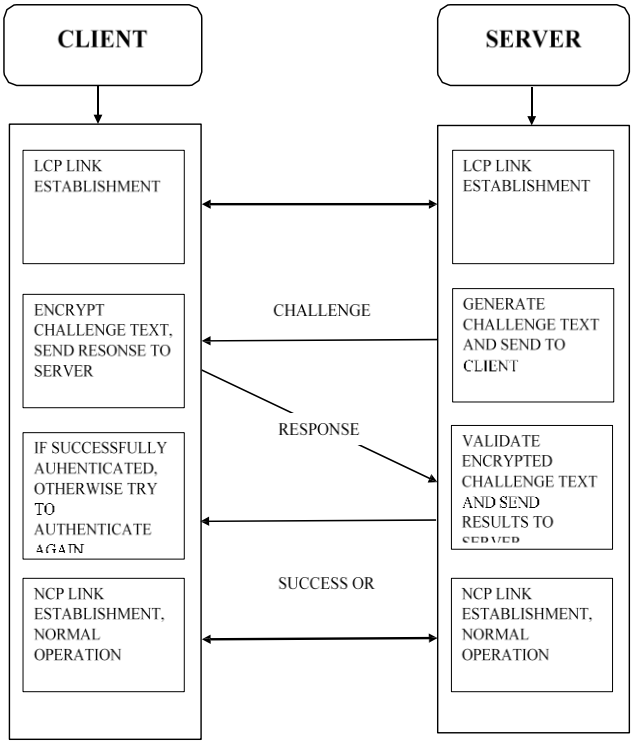

Figure 5. CHAP 3-way Handshake

5. AUTHENTICATION METHODS

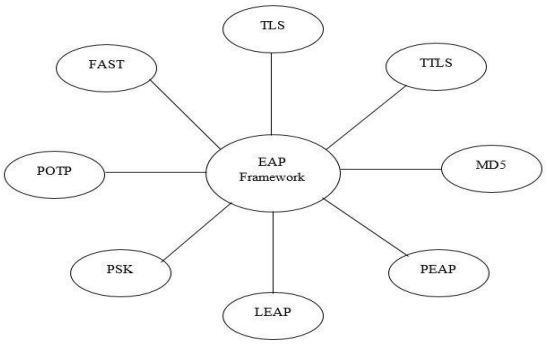

Figure 6. EAP Authentication Methods

The Figure 6. shows the various authentication methods that can be implemented in the EAP framework. Each of them is briefly defined in this section.

5.1 EAP-TLS

EAP-TLS (Transport Level Security) is an EAP method that based on RFC 2716. It uses public key infrastructure (PKI) digital certificate for the supplicant and the authentication server to provide mutual authentication between them. PKI certificate will contain information about the name of the server or user"s information. This gives a means for mutual authentication between the client and the authenticator and between the authenticator and the client. It dynamically generates and distributes user-based and session-based encryption keys to secure connections. EAP-TLS is considered to be very secure. EAP-TLS resists most attacks, such as replay and MITM attacks. The main features provided by EAP–TLS are key exchange and establishment, mutual authentication, support for the fragmentation and reassembly, and fast reconnect.

5.2 EAP-TTLS

EAP-TTLS is described in RFC 5281. It is an extension of EAP-TLS that eliminates PKI digital certificate and reduces the complexity of implementing TLS. The authentication process takes place inside the secure tunnel in which the protection of the authentication methods which validate the client is done. After the verification of client is done the tunnel gets collapsed. Then data exchange takes place using a less secure EAP method, such as another legacy method of authentication

or MD5, such as PAP or CHAP. It permits the use of legacy password-based protocols with existing authentication databases, while protecting the security of these legacy protocols against man in the middle and eavesdropping attacks.

5.3 EAP-MD5

EAP-MD5 is described in RFC 2284. It is a challenge response handshake protocol. It uses a one-way hash algorithm in combination with a shared secret and a challenge to verify the knowledge of supplicant about the shared secret. When a user creates his/her account on server and type password then server takes hash of that password and stores it. Next time when user want to login to the server then user have to enter the password. The MD5 protocol on client side converts that password into hash value and forwards it to server. Now server receives the hash from client. A comparison is done based on the hash values it gets from client and stored at server and accordingly result is out. MD5 is implemented easily then the other protocols which make it more user friendly. With just client side authentication, EAP-MD5 is also vulnerable to Man-In-The- Middle attacks. It also suffers from different type of attack like reply attack, birthday attack, dictionary attack etc.

5.4 EAP-PEAP

EAP-PEAP is similar to TLS. It uses private key infrastructure (PKI) digital certificates to authenticate. Unlike TLS, EAP-PEAP requires a single certificate to authenticate. It is a one-way authentication method. There is a reduction in the cost and complexity by only requiring certificates to be present on the authenticator, not on the clients. PEAP can be useful in message encryption, secure key exchange and fast reconnect.

5.5 EAP-LEAP

Lightweight EAP (LEAP) is also known as Cisco-EAP. It is a method defined by Cisco Systems. LEAP offers mutual authentication instead of a one-way authentication between supplicant and AS. 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 stores at client then server is valid. Similarly, server also verifies the client by similar method so by this mutual authentication is achieved. This feature eliminates the MITM attacks by rogue APs. LEAP is vulnerable to dictionary attacks. 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.

5.6 EAP-POTP

EAP Protected One-Time Password (EAP-POTP) described in RFC 4793, is an EAP method developed that uses one- time password (OTP) to generate authentication keys. It provides unilateral or mutual authentication for methods using EAP. It uses two-factor user authentication, requiring an OTP access and knowledge of a personal identification number (PIN) to perform authentication.

5.7 EAP-PSK

EAP Pre-shared key (EAP-PSK) is described in RFC 4764. It uses a pre-shared key for mutual authentication and session key derivation. If mutual authentication is successful, then a secure communication channel is created for both the entities to communicate and authenticate over insecure networks such as IEEE 802.11. EAP-PSK provides a lightweight and extensible EAP method that does not require any public-key cryptography. The message exchange is done in a minimum of four messages.

6. RELATED WORK

Baqer et al., [3] proposed an offline payment protocol SMAPs (Short Message Authentication Protocols) for areas having inconsistent or no network connections. It was designed keeping in view the less developed countries. It maximized usability in offline transactions by reducing the number of digits a user has to speak, hear and type, while providing robust recovery mechanisms for the inevitable errors and making sure there isn"t any scalable attack that is large enough to care about. The protocol can also enable payment networks to support delay-tolerant authentication. Mitchell et al., [4] designed a lightweight, flexible authentication protocol EAP-GPSK based on symmetric cryptography and pre-shared key. It was developed under the IETF EAP Method Update(EMU) working group. The protocol reduced the number of round trips and is well suited for devices having limited resources and memory. They used a finite-state model to find errors and Protocol Composition Logic to prove correctness after error finding and repairing. It also allows the negotiation of cryptographic cipher suites which detail the encryption algorithm (if any), the message integrity mechanism and the key derivation algorithm the protocol participants will use.

LiPing Du et al., [5] presented a micro-certificate based authentication protocol, which is lightweight and can be used on the internet and in the internet of things. This authentication mechanism uses the less authentication parameters to form the micro-certificate for the authentication protocol and CPU security chip is used to store the important secret information. The security is improved because of the dynamic nature of micro certificate used. It used the symmetric

cryptographic algorithms, CSK technology and cipher chip technology to realize the authentication. As compared with other authentication protocols, it has the advantage of small size, fast speed and high security.

Sonal Fatangare and Archana Lomte [6] proposed an OTP based user authentication protocol which provides a way to resist password stealing, password reuse ad collision attack. SWAP (Secure Web Authentication Protocol) is efficient and affordable compared with the conventional web authentication mechanism. The design principle is to eliminate the negative influence of human factor as much as possible. It only requires each participating website possess a unique phone number and involves a registration and a recovery phase. Through SWAP, each user only needs to remember a long-term password which is used to protect cell phone. Users are free from typing any passwords into untrusted computers for login on all websites.

P. Pacyna and R.Chrabaszcz [7] introduced an extension to EAP. the EAP Re-Authentication Protocol (ERP), which aims to overcome the authentication latency during handoff. The ERP protocol introduces fast re-authentication in just one message round trip time, using less computation power than required in a typical EAP exchange. EAP Re- authentication server (ER) is the new element in the EAP framework. It serves as a local proxy to AAA server. It provides new protocol features, specifically the protocol extensions and the new key management framework indeed reduce signaling overhead, offload the server and improve security on the wireless link.

KirtiRaj Bhatele et al. [8] introduced a hybrid security protocol using a combination of both type of cryptographic algorithms in order to enhance security. In this hash value of the decrypted message is calculated using MD5 algorithm. This hash value is encrypted with dual RSA and the encrypted message of this hash value is also sent to destination. Now at the receiving end, hash value of decrypted plaintext is calculated with MD5 and then it is compared with the hash value of original plaintext which is calculated at the sending end for its integrity. By this we are able to know whether the original text is being altered or not during transmission in the communication medium.

Xiumei Liu et al., [9] proposed a key exchange protocol for group called as nPAKE. Liu found that there is a large number of message exchange to server and that greatly increases the traffic on to the server. nPAKE reduces the traffic at the server. nPAKE is based on chosen based Diffie- Hellman assumption. Various analysis of this model shows that this protocol has some advantage in terms of traffic generated at the server and can resist many familiar attacks.

Bahareh Shojaie et al., [10] proposed a new methodology to implement EAP-TLS using Elliptical Curve Digital Signature Algorithm (ECDSA) and SHA-256 to provide enhanced performance and security. They compared it with the existing EAP-TLS method which used RSA signatures and SHA-1 to show faster response time and reduced turnaround time. Memory usage remains the same but security and efficiency gets increased. New methods provide a balance between security and optimized uses of resources and time.

Asokan et al., [11] proved that when an authentication protocol at the client is tunneled within another protocol, it is necessary for every last entity to show their participation in both protocols and if not done then the whole authentication is susceptible to man-in-the-middle attack. These type of protocols are constructed by combination of two protocols: an authentication and a tunnel protocol. A cryptographic binding facility is required between the tunnel protocol and the authentication protocol. A secret key is required by the authentication protocol for the use of the binding. With or without cryptographic binding, the protocol is vulnerable to dictionary attacks like man-in-the-middle.

Umesh Kumar et al., [12] overviewed the EAP framework which consists of different types of protocols. Some of the commonly used EAP authentication methods are also discussed. A secure authentication approach based on OTP considering the sending of OTP to the user in a more secure way so that any intruder might not get the access to the assets.

Umesh Kumar and Sapna Gambhir [13] proposed an authentication method E-EAP. It is not susceptible to reuse attack. In this protocol, email and SMS were used to deliver the password to the user to enhance the security. SHA-1 was used to generate passwords decreasing the chance of guessing the password. The password was split into two halves and sent via email and SMS. Both passwords are combined to get the password to use for login into the system.

Umesh Kumar et al.,[14] proposed a new key distribution using mobile agent based approach and authentication using fingerprint approach. The various previously described approaches were compared with the proposed approach to get the benefits of the mobile agent approach. Permanent keys are not transmitted so no eavesdropping takes place. The privacy of cancelable template can be done using one-way transformation. Integration of KDC and biometric with mobile agents provides high security protocol.

In the table below, comparisons are made between various authentication protocols implemented by several researchers. Several researchers have done quite a lot work in this domain and gave important conclusions. The benefits of using a particular protocol and drawbacks if implemented that protocol are discussed in the table.

Table 1. Comparison of Authentication Protocols

Reference No.	Protocol Implementation	Advantages	Disadvantages
1.	SMAP	Shorter authentication codes Transaction chaining possible Offline Capability Delay-tolerant network handling	False positive results using BAN logic
2.	EAP GPSK	Flexible Lightweight Usage of symmetric cryptography Minimizes no. of round trips	Denial-of-service Attack Non-standard derivation of master key Cipher suite downgrade attack
3.	Micro certificate authentication	Symmetric cryptography Small certificate size High Speed Fast Security	Cost of deployment is higher
4.	SWAP	Unique OTP Phishing Protection Password Reuse Prevention	SMS delay decreases performance Eavesdropping
5.	EAP Re-authentication Protocol	Overcomes handoff latency, Signal messages reduced Offloads the server Low CPU usage	Key management can be complex
6.	Hybrid security protocol	Smaller key size Shorter Response Time	Both symmetric and asymmetric cryptography use

7. CONCLUSION

In this paper, an overview of authentication protocols, its factors and various techniques that can be implemented in this domain is presented. The paper also covers the commonly used EAP framework and its various methods involved and their various advantages and disadvantages. The articles provided in the literature survey contributes to the many security related fields that uses authentication protocol techniques for various real-world applications. The overview just described above is of great importance and will help a developer to decide which framework/methods to choose. With this review, expecting to encourage future work in the domain.

8. REFERENCES

[1] Yogita Borse and Irfan Siddavatam. “A Novel Secure Remote User Authentication Protocol using Three Factors”, International Journal of Computer Applications, vol. 87, no. 17, pp. 1-6, February 2014.

[2] Dwiti Pandya, Ram Narayan, Sneha Thakkar, Tanvi Madhekar and Bhushan Thakare “An Overview of Various Authentication Methods and Protocols”, International Journal of Computer Applications, vol. 131, no. 9, pp. 25-27, 2015.

[3] Khaled Baqer, Johann Bezuidenhoudt, Ross Anderson and Markus Kuhn, “SMAPs: Short Message Authentication Protocols”, pp. 119-132, 2017.

[4] JC Mitchell, A Roy, P Rowe and A Scedrov “Analysis of EAP-GPSK authentication protocol”, International Conference on Applied Cryptography and Network Security, pp. 309-327, 2008.

[5] Li Ping Du and Jian WeiGuo Ying Li, "Research on Micro-Certificate Based Security System for Internet of Things", Applied Mechanics and Materials, vol. 263, pp. 3125-3129, 2013.

[6] Sonal Fatangare and Archana Lomte, “SWAP: Secure Web Authentication Protocol on Windows Mobile App”, International Journal of Computer Science and Mobile Computing, vol. 3, no. 6, pp. 674–680, 2014.

[7] P. Pacyna and R. Chrabąszcz, "Evaluation of EAP re-authentication protocol", 17th International Telecommunications Network Strategy and Planning Symposium (Networks), Montreal, pp. 45-49, 2016.

[8] K. Bhatele, A. Sinhal and M. Pathak, "A novel approach to the design of a new hybrid security protocol architecture," IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, pp. 429-433, 2012.

[9] Xiumei Liu, Junjiang Liu and Guiran Chang, "nPAKE: An Improved Group PAKE Protocol", IEEE Ninth Web Information Systems and Applications Conference, 2012.

[10] Bahareh Shojaie, Iman Saberi, Mazleena Salleh, Mahan Niknafskermani and Seyyed Morteza Alavi, "Improving EAP-TLS Performance Using Cryptographic Methods", International conference on computer & Information Science 2012.

[11] N. Asokan, Vaitteri Niemi and Kaisa Nyberg "Man-in-the Middle in Tunneled Authentication Protocols" Nokia Research Centre, Finland, 2002.

[12] Umesh Kumar, Praveen Kumar and Sapna Gambhir, "Analysis and Literature Review of IEEE 802.1x(Authentication) Protocols", International Journal of Engineering and Advanced Technology, vo. 3, no. 5, pp. 163-168, 2014.

[13] Umesh Kumar and Spana Gambhir, "Secured Authentication Method for Wireless Networks", IOSR Journal of Computer Engineering, pp.1-11, 2015.

[14] U. Kumar and S. Gambhir, "A novel approach for key distribution through fingerprint based authentication using mobile agent," 3rd International Conference on Computing for Sustainable Global Development, New Delhi, pp. 3441-3445, 2016.