Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P) Vol.7, No.2, 2018, pp.57-60
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajes-2018.7.2.2160

An Importance of the Authentication Mechanisms in the Networks: A Literature Survey

D. Selvamani[1] and V Selvi[2]
[1]Assistant Professor, Department of Computer Science, SIVET College, Gowrivakkam, Chennai, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India
E-Mail: selvamani.bhaskar@gmail.com, selvigiri.s@gmail.com

(Received 23 August 2018; Revised 15 September 2018; Accepted 3 October 2018; Available online 10 October 2018)

***Abstract*- Security is very important for any kind of networks. As a main communication mode, the security mechanism for multicast is not only the measure to ensure secured communications, but also the precondition for other security services. Attacks are one of the biggest concerns for security professionals. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies. This paper presents a brief survey on the authentication mechanisms in the networks for ensuring the security in various domains.**

***Keywords:* Network security, Authentication, Encryption, Decryption, Cloud, Big Data, Internet of Things, Ad Hoc Networks**

I. INTRODUCTION

Computer industry has created an array of identification and authentication technologies like userID/Passwords, One Time Password, Biometrics, Smartcards, Secure Socket Layer, Lightweight Directory Access Protocol, Security Assertion Markup language (SAML), OpenID and CardSpace address varying business and security requirements [1]. Each organization adopts one or more of these technologies to secure information against misuse and un-authorized access. In a networked environment, users are granted access to the network only when they provide their access information (e.g. User name & password) securely to check and validate their identity. If a person can prove that he is, also knows something that only he could know, it is reasonable to think that a person is he who claims to be. The purpose of personal authentication is to ensure that the rendered services are being accessed only by a legitimate user. All Network users aim to access information and transfer data safely. To make certain secure transmission of information between the parties; a group of challenges must.

II. IMPORTANCE OF NETWORK SECURITY

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well- developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered

1. *Access:* Authorized users are provided the means to communicate to and from a particular network.
2. *Confidentiality*: Information in the network remains private.
3. *Authentication*: Ensure the users of the network are who they say they are.
4. *Integrity*: Ensure the message has not been modified in transit.
5. *Non-Repudiation*: Ensure the user does not refute that he used the network.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack.

III. LITERATURE SURVEY ON AUTHENTICATION MECHANISMS FOR VARIOUS DOMAINS IN THE YEAR 2013 – 2018

Yao, Xuanxia, *et al.*,[1] revised the original Nyberg's fast one-way accumulator and constructs a lightweight multicast authentication mechanism for small scale IoT applications.

Lai, Chengzhe, *et al.*,[2] proposed a secure and efficient Authentication and Key Agreement (AKA) protocol, called SE-AKA, which can fit in with all of the group authentication scenarios in the LTE networks. Specifically, SE-AKA uses Elliptic Curve Diffie-Hellman (ECDH) to realize KFS/KBS, and it also adopts an asymmetric key cryptosystem to protect users' privacy.

Saman Taghavi Zargar [3] explored the scope of the DDoS flooding attack problem and attempts to combat it. It categorized the DDoS flooding attacks and classifies existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks.

Kothmayr, Thomas, *et al.*,[4] proposed security scheme is therefore based on RSA, the most widely used public key cryptography algorithm. It is designed to work over standard communication stacks that over UDP/IPv6 networking for Low power Wireless Personal Area Networks (6LoWPAN).

Hu, Chunqiang, *et al.*, [5] developed the Fuzzy Attribute-Based Signcryption (FABSC), a novel security mechanism that makes a proper tradeoff between security and elasticity.

Jiliang Zhou[6] proposed an efficient and secures routing protocol based on encryption and authentication for WSNs. BEARP especially mitigates the loads of sensor nodes by transferring routing related tasks to BS, which not only maintains network wide energy equivalence and prolongs network lifetime but also improves the security mechanism performed uniquely by the secure BS.

Debiao He [7] proposed a biometrics-based authentication scheme for multiserver environment using elliptic curve cryptography.

Pawani Porambage[8] proposed a pervasive lightweight authentication and keying mechanism for WSNs in distributed IoT applications, in which the sensor nodes can establish secured links with peer sensor nodes and end-users.

Mian Ahmad Jan[9] proposed a lightweight mutual authentication scheme which validates the identities of the participating devices before engaging them in communication for the resource observation.

Ren´eHummen[10] presented a comprehensive, yet compact solution for authentication, authorization, and secure data transmission in the IP-based IoT.

Pawani Porambage [11] proposed an implicit certificate-based authentication mechanism for WSNs in distributed IoT applications. The developed two-phase authentication protocol allows the sensor nodes and the end-users to authenticate each other and initiate secure connections.

Soobok Shin[12] proposed a lightweight authentication scheme. Also, the scheme ensures user's anonymity and provides secure password update, session key agreement, and mutual authentication between entities to resist to possible attacks in ubiquitous networks.

Imran Memon[13] proposed the prevent user private information and secure communication by asymmetric cryptography scheme. The authors solved the wireless communication problem in A3 algorithm such as eavesdropping and this problem solved by asymmetric cryptography scheme because of its robustness against this type of attack by providing mutual authentication make the system more secure.

ProsantaGope [14] propose an improved protocol of Wen *et al.*, [15] which can immune to various known types of attacks like forgery attack, replay attack, known session key attack, backward and forward secrecy etc.

Qi Jiang [16] proposed improved authentication protocol, which inherits the merits of the scheme of Chen *et al.*, [17] and is free from the security flaw of their scheme. Chen *et al.*,proposed a smart-card-based password authentication scheme and claimed that the scheme can withstand offline password guessing attacks even if the information stored in the smart card is extracted by the adversary.

Neeraj Kumar[18] proposes an intelligent RFID-enabled authentication scheme for healthcare applications in vehicular cloud computing (VCC) environment. In the proposed scheme, a Petri Nets-based authentication model is used for authentication of tags, and readers. Both server, and tag authentications are protected by strong elliptical curve cryptography (ECC)-based key generation mechanism.

Zheng Yan [19] proposed framework applies adaptive trust evaluation and management technologies and sustainable trusted computing technologies to ensure computing platform trust and achieve software-defined network security.

SaruKumari [20] an enhanced trust-extended authentication scheme for VANET is proposed. It also enhanced the performance of the authentication process using transitive trust relationship among vehicles.

Adnan Ahmed[21] presented a Trust and Energy aware Secure Routing Protocol (TESRP) for WSN that exploits a distributed trust model for discovering and isolating misbehaving nodes.

Khalid Mahmood[22] proposed a hybrid Diffie–Hellman based lightweight authentication scheme using AES and RSA for session key generation. To ensure message integrity, the advantages of hash based message authentication code are exploited.

Chengzhe Lai[23] introduced a novel lightweight group authentication scheme for resource-constrained M2M Group-based Lightweight Authentication Scheme for Resource-constrained Machine to Machine

Communications (GLARM) under the 3GPP network architecture, which consists of two protocols that can achieve efficient and secure group authentication in the 3GPP access case and non-3GPP access case, respectively.

KlimisNtalianis [24] proposed a robust authentication mechanism based on semantic segmentation, chaotic encryption, and data hiding.

Jaewook Jung [25] presented a detailed analysis of the security and performance of proposed authenticated key agreement mechanism, which not only enhances security compared to that of related schemes, but also takes efficiency into consideration.

Xiong Li[26] a lightweight anonymous mutual authentication and key agreement scheme for the centralized two-hop Wireless Body Area Network (WBANs) is proposed in this paper, which allows sensor nodes attached to the patient's body to authenticate with the local server/hub node and establish a session key in an anonymous and unlinkable manner.

Kakelli Anil Kumar [27] proposed a new secure multipath routing protocol (NSRP) for military heterogeneous wireless sensor network (MHTWSN) for secure data transmission. NSRP uses elliptic curve cryptography (ECC) to discover trusted neighbor nodes and establish the secure multiple routes for reliable data delivery in MHTWSN.

Pandi Vijayakumar[28] introduced a novel approach to improve the existing authentication support to VANETs. In this proposed framework, first an anonymous authentication approach for preserving the privacy is proposed which not only performs the vehicle user's anonymous authentication but preserves the message integrity of the transmitting messages as well.

Parwinder Kaur Dhillon[29] a lightweight biometric based remote user authentication and key agreement scheme for secure access to IoT services has been proposed. The protocol makes use of lightweight hash operations and XOR operation.

Jian Shen[30] proposed a cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks.

Xiong Li[31] proposed a three-factor anonymous authentication scheme for WSNs in Internet of Things environments, where fuzzy commitment scheme is adopted to handle the user's biometric information.

Fushan Wei [32] proposed an anonymous authentication scheme for Wireless Body Area Networks (WBANs) based on low-entropy password and prove its security in the random oracle model.

Samet Tonyali[33] propose new protocols to adapt Fully Homomorphic Encryption (FHE) and secure MultiParty Computation (MPC) to be deployed in Smart Grid (SG) Advanced Metering Infrastructure (AMI) networks that are formed using wireless mesh networks. The proposed protocols conceal the smart meters' (SMs) reading data by encrypting it (FHE) or computing its shares on a randomly generated polynomial (secure MPC).

SravaniChalla [34] proposed scheme supports functionality features, such as dynamic sensor node addition, password as well as biometrics update, smart card revocation along with other usual features required for user authentication in wireless sensor networks.

Jianbing Ni[35] propose an efficient and secure service oriented authentication framework supporting network slicing and fog computing for 5G-enabled IoT services.

SK Hafizul Islam[36] presented a password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) protocol for VANETs. This protocol offers group-key generation, user leaving, user join, and password change facilities.

Mohamed M. Mansour[37] proposed a secure mutual authentication scheme with perfect forward-secrecy for WSN. Likewise, provides resilience against various types of known attacks in WSNs.

IV. NEED OF AUTHENTICATION MECHANISMS FOR NETWORKS

Using of authentication mechanism lead to address the following problems. The definition problems are given below:

1. *Authentication:* Authentication means enabling the network to only admit the authorized users to have access to its resources. It provides the way where the claimed identifier is verified by the access control mechanisms through some means.
2. *Access Control:* The discipline in which mechanisms and policies are established that restrict access to the computer resources only to correct users.
3. *Identification:* It is a way where a resource claims (or is identified through other means) a specific and unique identifier.
4. *Authorization:* Which determines the privileges associated with authenticated identity.
5. *Security:* The ability of a system to protect data, services and resources against misuse by unauthorized users.
6. *Privacy:* The ability of a system to protect then identity and location of its users from un-authorized disclosure.

V. CONCLUSION

In this paper, we have evaluated many researchers' approaches for network security in WSN, IoT, Cloud Computing, WBAN, and Big Data. This article suggests a research area in the authentication domain of security threats for WSN, WBAN, Cloud computing, IoT. In future smart home conditions, there will be multi-modal sensor explications that include the advantages reported. However, there are still problems to surmount to perform these pervasive context-aware applications.

REFERENCES

[1] Yao, Xuanxia, *et al.,* "A lightweight multicast authentication mechanism for small scale IoT applications", *IEEE Sensors Journal,* Vol.13, No. 10, pp. 3693-3701, 2013.

[2] Lai, Chengzhe, *et al.,* "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks", *Computer Networks,* Vol.57, No. 17, pp.3492-3510, 2013.

[3] Zargar, SamanTaghavi, James Joshi and David Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks", *IEEE Communications Surveys & Tutorials,* Vol.15, No. 4, pp.2046-2069, 2013.

[4] Kothmayr, Thomas, *et al.,* "DTLS based security and two-way authentication for the Internet of Things", *Ad Hoc Networks,*Vol.11, No. 8, pp.2710-2723, 2013.

[5] Hu, Chunqiang, *et al.,* "Body area network security: a fuzzy attribute-based signcryption scheme", *IEEE Journal on Selected Areas in Communications,* Vol.31, No. 9, pp.37-46, 2013.

[6] Zhou, Jiliang, "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks", *International Journal of Distributed Sensor Networks,* Vol.9, No. 4, pp. 108968, 2013.

[7] He, Debiao and Ding Wang, "Robust biometrics-based authentication scheme for multiserver environment", *IEEE Systems Journal*, Vol.9, No. 3, pp.816-823, 2015.

[8] Porambage, Pawani, *et al.,* "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications",*International Journal of Distributed Sensor Networks,*Vol.10, No. 7, pp. 357430, 2014.

[9] Jan, Mian Ahmad, *et al.,* "A robust authentication scheme for observing resources in the internet of things environment", *Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 13th International Conference, IEEE,* 2014.

[10] Hummen, René, *et al.,* "Delegation-based Authentication and Authorization for the IP-based Internet of Things", *Sensing, Communication* and *Networking (SECON), 2014 Eleventh Annual IEEE International Conference IEEE,*2014.

[11] Porambage, Pawani, *et al.,* "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications",*Wireless Communications and Networking Conference (WCNC), IEEE,* 2014.

[12] Shin, Soobok, HongjinYeh and Kangseok Kim, "An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks", *Peer-to-peer Networking and Applications,* Vol. 8, No. 4, pp. 674-683, 2015.

[13] Memon, Imran, *et al.,* "Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme",*Wireless PersonalCommunications,* Vol. 84, No. 2, pp. 1487-1508, 2015.

[14] Gope, Prosanta and Tzonelih Hwang, "Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks", *Wireless Personal Communications,* Vol. 82, No. 4, pp. 2231-2245, 2015.

[15] Wen, Fengtong, Willy Susilo and Guomin Yang, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks", *Wireless personal communications,* Vol. 73, No. 3, pp. 993-1004, 2013.

[16] Jiang, Qi, *et al.,* "Improvement of robust smart-card-based password authentication scheme", *International Journal of Communication Systems,* Vol. 28, No. 2, pp. 383-393, 2015.

[17] Chen, Bae-Ling, Wen-Chung Kuo and Lih-ChyauWuu, "Robust smart-card-based remote user password authentication scheme", *International Journal of Communication Systems,* Vol. 27, No. 2, pp. 377-389, 2014.

[18] Neeraj Kumar, *et al.,* "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud",*Peer-to-Peer Networking and Applications,* Vol. 9, No. 5, pp. 824-840, 2016.

[19] Yan, Zheng, Peng Zhang and Athanasios V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking",*Security and communication networks,* Vol. 9, No. 16, pp. 3059-3069, 2016.

[20] Kumari, Saru, *et al.,* "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks", *Security and Communication Networks,* Vol. 9, No. 17, pp. 4255-4271, 2016.

[21] Ahmed, Adnan, *et al.,* "A secure routing protocol with trust and energy awareness for wireless sensor network",*Mobile Networks and Applications,* Vol. 21, No. 2, pp. 272-285, 2016.

[22] Mahmood, Khalid, *et al.,* "A lightweight message authentication scheme for Smart Grid communications in power sector", *Computers & Electrical Engineering,* Vol. 52, pp. 114-124, 2016.

[23] Lai, Chengzhe, *et al.,* "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications", *Computer Networks,* Vol. 99, pp. 66-81, 2016.

[24] Ntalianis, Klimis and Nicolas Tsapatsoulis, "Remote authentication via biometrics: A robust video-object steganographic mechanism over wireless networks", *IEEE Transactions on Emerging Topics in Computing,* Vol. 4, No. 1, pp. 156-174, 2016.

[25] Jung, Jaewook, *et al.,* "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks",*Sensors,* Vol. 17, No. 3, pp. 644.

[26] Li, Xiong, *et al.,* "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks",*Computer Networks,* Vol. 129, pp. 429-443, 2017.

[27] Kumar, Kakelli Anil, Addepalli V. N. Krishna and K. ShahuChatrapati, "New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks", *Journal of Information and Optimization Sciences,* Vol. 38, No. 2, pp. 341-365, 2017.

[28] Vijayakumar, Pandi, *et al.,* "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks",*Cluster Computing,* Vol. 20, No. 3, pp. 2439-2450, 2017.

[29] Dhillon, ParwinderKaur and SheetalKalra, "A lightweight biometrics based remote user authentication scheme for IoT services",*Journal of Information Security and Applications,* Vol. 34, pp. 255-270, 2017.

[30] Shen, Jian, *et al.,* "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks",*Journal of Network and Computer Applications,* Vol. 106, pp. 117-123, 2018.

[31] Li, Xiong, *et al.,* "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments",*Journal of Network and Computer Applications,* Vol. 103, pp. 194-204, 2018.

[32] Wei, Fushan, *et al.,* "A provably secure password-based anonymous authentication scheme for wireless body area networks",*Computers & Electrical Engineering,* Vol. 65, pp. 322-331, 2018.

[33] Tonyali, Samet, *et al.,* "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems",*Future Generation Computer Systems,* Vol. 78, pp. 547-557, 2018.

[34] Sravani Challa, *et al.,* "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks", *Computers & Electrical Engineering,* Vol. 69, pp. 534-554, 2018.

[35] Jianbing Ni, Xiaodong Lin and Xuemin Sherman Shen, "Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT", *IEEE Journal on Selected Areas in Communications,* Vol. 36.3, pp. 644-657, 2018.

[36] SK Hafizu Islam, *et al.,* "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs", *Future Generation Computer Systems,* Vol. 84, pp. 216-227, 2018.

[37] Mohamed M. Mansour, Fatty M. Salem and Elsayed M. Saad, "A Secure Mutual Authentication Scheme with Perfect Forward-Secrecy for Wireless Sensor Networks", *International Conference on Advanced Intelligent Systems and Informatics, Springer, Cham,* 2018.