rnational Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Survey of Authentication Framework for the Physical Objects in WSN of IoT

Chandrakant R. Mankar[1], Dr. Vinod M. Patil[2], Gopal P. Gawali[3]

[1]Research Scholar, Department of Computer Science, Shri Shivaji College, Akola, Maharashtra, India

[2]Research Guide, Department of Computer Science, Shri Shivaji College, Akola, Maharashtra, India

[3]Assistant Professor & Head, Department of Computer Science, R. A. College Washim, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 03 June 2023
Published: 17 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
507-512

ABSTRACT

In IoT proliferation of the WSN is rapid, to ensure the security of the physical objects many challenges are faced. This paper is a comprehensive survey of frameworks for authentication that are being proposed on different parameters, provides detailed analysis of techniques and protocols required for authentication framework. The survey explores authentication framework components like digital signatures, certificates, different encryption schemes of keys, and offers new researchers designers of systems to understand the different approaches in developing the efficient and robust solution for physical objects authentication framework.

Keywords: Authentication, Authorization, Physical Objects, IoT, WSN, PUF, Block-chain, Encryption, Integrity.

I. INTRODUCTION

Millions of physical objects communicate to each-others using the IoT, through various application like Smart Health [20], Smart Room, Smart Homes, Smart Cities and Smart Grid. Authentication is one of the main aspect of security in IoT [16]. As the security of the physical objects is critical issue but their authentication while communication is the key concern. The physical objects over the WSN are new to each-others, while communication their authentication needs to be done in order to create trust for communication across the WSN of IoT [1-5]. As one of the application of IoT is Health care devices the authentication becomes necessary component as it can risk to life of the patient wearing the IoT health devices which are continuously monitoring [19].Various Researchers have proposed their research through their study and articles, some them are discussed in the section 2.

1.1 **Authentication Framework:** Authentication in IoT is a one of the crucial mechanism for security in IoT. The physical objects like IoT devices and user needs access to the resources so their identity must be authenticated before granting the access.

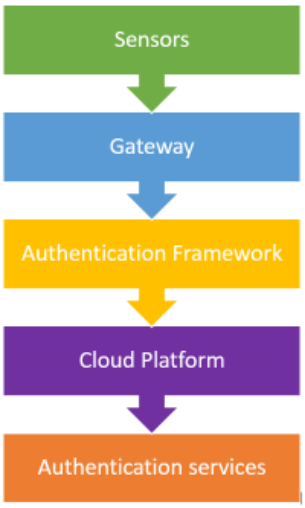

Fig. 1 Framework for authentication of Physical Objects [17]

There are many authentication framework mechanisms being proposed some of them are discussed below:

- Sensors: Sensors are the components that are Physical objects.
- Gateway: The gateway acts as interface between the physical objects and system.
- Authentication Frame work: This ensures authentication of physical objects.
- Cloud Platform: Cloud platform are used to serve storage for the data.
- Authentication services: This handles process of authentication.

a) ABE: Attribute Based Encryption, this scheme is powerful, scalable and flexible for encryption, encrypts and decrypts the data according to the user assigned attributes. The attributes are assigned to the physical objects and user data, according to the policy. During this encrypted ciphertext is the policy, which is decrypted by the user.[24]

b) ECC: Elliptic Curve Cryptography, in this scheme elliptic curves are used in cryptography algorithm, it avoids numbers in generation of keys to be shared. [25]

c) IBC: Identity Based Cryptography, here the key generator center is used for key distributions,[26]

d) IBE: Identity Based Encryption, this scheme use public key & private key given by third party for the encryption and decryption of the message. Here the digital signature/certification schemes can be used for the key depending on users identity.[27]

e) LAP: Light-Weight Authentication Protocol are required for the low processing IoT devices which are running on less number of resources. Due to small in size these kind of IoT devices are being manufactures on large scale and are available at cheaper prices.

f) PKI: Public Key Infrastructure is used to generate public keys so as to share and use them in encryption for authentication of physical devices, usually done by the third party.

1.2 Authentication Protocols:

Authentication Protocols are required for the authentication as a parameters to strengthen systems some of the commonly used protocols in IoT are discussed below [7-8]:

Table 1:Common Authentication protocols

Authentication Protocols	Description
Biometrics	For authentication it uses physical/behavioral characteristics
Physical Tokens	To authenticate by using physical objects as a factor
OAuth 2.0	Used for authentication and authorization in API's
OpenID connect	Used on top of OAuth 2.0 for authentication and authorization
Kerberos	Used for authentication, encryption and integrity with help of symmetric key cryptography
IPSec	Used in authentication and encryption in IP networks.

II. Literature Survey

M. Alizadeh, et. al. [6] focuses on the WSN, ensuring the authentication, suggested secure ticket- based scheme for the authentication. This scheme is of three phases: authenticating while registering sensor, login and authentication. The proposed method used disposable tickets while authenticating the gateway and nodes mutually to prevent impersonating attack, protecting the privacy of node, the proposed scheme is analyzed using BAN logic, consuming less time while performing cryptographic operations. The tickets are generated using authentication server, contains time stamp, session key and public key of the device. The efficiency and security of the proposed method when compared with others is claimed by the author.

A. M. Ansari, et. al. [9] propose a lightweight secure middleware based framework for the authentication of node, to improve authentication, management of identity and trust for nodes communicating securely. In this scheme, introduces middleware to be resourceful mechanism for authentication, which acts as gateway where the nodes are authenticated them while accessing in the network. The scheme follows: registration phase where the used and node register and get identity, authentication phase to adopt notion, where user sent message for authentication for the target node, node addition phase where the additional nodes are introduced so that system keeps working while some nodes stop working due to suffering from hardware failure, dead battery problems. Here the session key along with public key is used in encryption.

M. Barbareschi, et. al.[10] presents dPheMAP mechanism as a service for Fog IoT system, where mutual hardware authentication is performed using Physically Unclonable Functions (PUF's). PUF's are integrated with unique characteristics in the manufacturing process. Distribution of the authentication protocol for the fog devices, presented the chef automate framework based infrastructure of a real IoT devices. Detailed analysis of the proposed and existing authentication schemes is provided, claiming more secure and efficient. Paper addresses the Fog IoT systems and its challenges in security of it.

M. N. Aman, et. al.[11] focuses on authenticating using PUF's and a cryptography by lightweight symmetry as two factors, for safe guarding the IoT devices against the attacks, also use the RSSI, LQI for the verification of location of devices. In proposed scheme the devices goes through phase of registering device, authentication, mobility and CRP's. The comparative analysis done with the existing protocols shows the proposed system is more successful to secure IoT devices from impersonation, Device anonymity, DoS, cloning, physical, location proximity attacks.

T. Ahsan [13], presented technique to authenticate device, user and transaction using the blockchain scheme utilizing decentralized, GUI interface by removing the third party centralized scheme. Also provided analysis of the proposed system with existing systems. Uses OAuth technique for securing, describes architecture of proposed scheme with implementing hash-key algorithm with MySQL server using PHP, Addressing the attacks like Jamming, Sybil node, Man-in-the-middle, Insecure interface and double dependency with proposed system.

M. N. Aman [14] Using PUF in Mutual authentication, the author generates key for the physical objects also while addressing security challenges in IoT. The key is extracted from string of bit from PUF, also use digital certificates for the physical objects. The authentication server is based on cloud, used to store certificates.

B. Liu [15] proposed PPSI based method for IoT to ensure authentication of identity, here encryption is homomorphic along with garbled circuits. The data is encrypted using 2 keys and then transmitted to the circuit, which gives actual data, here circuit ensures identity of the user to be authenticated.

M.T. Al Ahmed [21] and K.H.Wang[2] proposed authentication scheme using hierarchical blockchain, here every physical object has self blockchain which is connected to master blockchain. This authentication

mechanism is based on challenge-response scheme, the encrypted response is added to the blockchain. The authenticity of the response is done by master blockchain.

M. Saquib [23] presents light weight three factor authentication framework aim to be secure against various attacks like brute force, impersonate. Here authentication parameters are biometric, pattern and password, which are then analyzed by the server.

Comparison of Authentication Framework

There are different authentication techniques which are implemented, some commonly used are compared in the following table [18, 22]:

Table 2: Authentication techniques

Framework for Authentication	Parameters used	Advantages	Remark
PKI	Public key , Private key, digital signatures/ certificates	Strong security for Authentication, encryption, confidentiality and integrity. It can be costly as it needs digital signature/certification.	Secure against Man-in-the-middle attack
Kerberos	Symmetric key, Key distribution center, ticket, Authentication server	Strong against IoT attacks like eavesdropping, replay.	Secure against eavesdropping, Impersonation attacks
ECC	Elliptic curves, public key, private key, digital signals	Small in size, faster in time. Needs to be care-full while selecting the parameters.	Secure against Quantum computing attacks
LAP	Challenge- response scheme	For less resourced system this can be implemented	Secure against eavesdropping and replay attack
OAuth 2.0	Token, ID	Simple, secure, flexible if implemented in correct way.	Secure against token replay attacks
SAML	Assertion, signature	Applicable for distributes systems, uses identity providers and service providers	Secure against spoofing attacks like identity spoofing

Blockchain mechanism is also one of the commonly used in parameter in authentication framework, as there are number of applications that are using Blockchain as one of the parameter for authentication.[19]

III. CONCLUSION

In WSN of IoT Framework for Authentication is crucial to ensure its security, we explored different authentication framework and their effectiveness. Our key findings are schemes having limited resources using password approaches lack in securing WSN, some cryptographic protocols are used as alternatives to these schemes. PKI and digital certificates show promising secure WSN, leveraging different key cryptography in ensuring security of WSN. Lightweight Authentication Protocols were ahead in securing WSN, they work on different algorithms like hashing. The Blockchain based authentication schemes were quit trustworthiness showing effective against malicious attacks, scalability of it needs to be studied.

We conclude that after understanding the security requirement of appropriate framework for authentication for WSN in IoT, a combination of lightweight and blockchain based framework can enhance security to WSN. For future researchers the aspect of research should be on addressing resource scalability and their operability in advancement in this field.

IV. REFERENCES

[1]. C. R. Mankar, Dr. Prof. V. M. Patil, G. P. Gawali, "Review of Attacks on Physical Objects and Their Countermeasures in WSN of IoT Framework", International Interdisciplinary Virtual Conference on 'Recent Advancements in Computer Science, Management and Information Technology', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 9,issue 7, March-April 2023.

[2]. M. A. Ferrag, K. A. Maglaras, et al., "Authentication Protocols for Internet of Things: A Comprehensive Survey", Security and Communication Networks, vol. 2017.

[3]. M. Trnka, T. Cerny, and N. Stickney, "Survey of Authentication and Authorization for the Internet of Things", Security and Communication Networks, vol. 2018.

[4]. K. O. Bate, N. Kumar, S. Khatri, "Framework for authentication and access control in IoT", 2nd International Conference on Telecommunication and Networks (Tel-NET) 2017.

[5]. M. El-hajj, A. Fadlallah, M. Chamoun, et. al., "A Survey of Internet of Things (IoT) Authentication Schemes", Sensors, 2019.

[6]. M. Alizadeh, M. H. Tadayon, A. Jolfaei, "Secure ticket-based authentication method for IoT applications", Digital Communications and Networks, 2021.

[7]. T. Nandy, et. al., "Review on Security of Internet of Things Authentication Mechanism", IEEE Access, vol. 7, 2019.

[8]. M. B. M. Noor, W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey", Computer Networks, 2018.

[9]. A. M. Ansari, Dr. M. Husain, "Middleware Based Node Authentication Framework For IoT Networks", Proceedings of the International Conference on Inventive in Computing Applications (ICIRCA-2018), 2018.

[10]. M. Barbareschi, et. al., "PUF-enabled Authentication-as-a-Service in Fog-IoT systems", IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2019.

[11]. M. N. Aman, M. H. Basheer, B. Sikdar, "Two-Factor Authentication for IoT Location Information", IEEE Internet of Things Journal, vol. 6, April 2019.

[12]. S. Kavianpour, et. al., "A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices", Hindawi Journal of Computer Networks and Communication, vol. 2019.

[13]. T. Ahsan, et. al., "IoT Devices, User Authentication, and Data Management in a Secure, Validated Manner through Blockchain System", Hindawi Wireless Communication and Mobile Computing, vol. 2022.

[14]. M. N. Aman, K. C. Chua and B. Sikdar, "Mutual Authentication in IoT System using Physical Unclonable Functions", IEEE Internet of Things Journal, vol. 4, Oct. 2017.

[15]. B. Liu, et. al., "SEPSI: A Secure and Efficient Privacy-Preserving Set Intersection with Identity Authentication in IoT", Mathematics, 2022.

[16]. R. S. M. Joshita, L. Arockiam, "Authentication in IoT Environment: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, Issue 10, 2016.

[17]. I. Ali, S. Sabir, Z. Ullah, "Internet of Things Security, Devices Authentication and Access Control: A Review", International Journal of Computer Science and Information Security (IJCSIS), vol. 14, Aug. 2016.

[18]. M. El-Hajj, et. al., "Analysis of authentication techniques in Internet of Things (IoT)", 1st Cyber Security in Networking Conference (CSNet), 2017.

[19]. U. Khalil, et. al., "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancement, Challenges and Future Research Directions", Survey, 2022.

[20]. A. H. Sodhro, et.al., "Intelligent authentication of 5G health devices: A survey", IEEE Internet of Things, vol. 20, 2022.

[21]. M. T. Al Ahmed, et. al., "Hierarchical blockchain structure for node authentication in IoT networks", Egyptian Informatics Journal, vol. 23, Issue 2, 2022.

[22]. K. H. Wang, et. al., "A secure authentication scheme for Internet of Things", Pervasive and Mobile Computing, vol. 42, 2017.

[23]. M. Saqib, B. Jasra, A. H. Moon, "A Lightweight three factor authentication framework for IoT based critical applications", Journal of King Saud University – Computer and Information Sciences, 2021

[24]. Li. Chongxuan, H. Zhang, Y. Mao, "A Survey of Attribute-Based Encryption Scheme", IEEE Access, vol. 8, 2020

[25]. M. I. Islam, et. al., "Elliptic Curve Cryptography for Wireless Sensor Networks: A Survey and Comparative analysis", Sensors, vol. 16, 2016.

[26]. F. Rahman, et. al., "A Survey on Identity-Based Cryptography", Future and Informatics Journal, vol. 6, 2021

[27]. S. Lu, X. Cheng, and J. Wang, "Efficient and secure revocable Identity-Based Encryption with Tight Security Reduction", IEEE Transactions on Dependable and Secure Computing, 2021.

Cite this article as :

Chandrakant R. Mankar, Dr. Vinod M. Patil, Gopal P. Gawali, "Survey of Authentication Framework for the Physical Objects in WSN of IoT", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.507-512, May-June-2023.