Computer Science

E-ISSN No : 2456-5040 | Volume : 10 | Issue : 11 | November 2025

EFFICIENT AUTHENTICATION FRAMEWORK FOR INTERNET OF THINGS

Vaidehi Shah[1], Dr. Vijaykumar B Gadhavi[2]

Access Online

Article DOI:
10.5281/zenodo.17839837

[1]Research Scholar,Computer Engineering Department Swaminarayan University, India
[2]Associate Professor & Dean –Faculty of Engineering, Computer Engineering Department, Swaminarayan University, India

How to Cite:
Vaidehi Shah, Dr. Vijaykumar B Gadhavi (2025), Efficient Authentication Framework for Internet of Things, International Educational Applied Scientific & Research Journal (IEASRJ), Vol: 10, Issue: 11, 11-19

ABSTRACT

This study explores both existing and emerging threats in IoT networks, including device exploitation, communication eavesdropping, malware dissemination, and large-scale distributed attacks. A detailed literature review is conducted to analyze current security mechanisms, recent research advancements, and evolving trends in IoT security.The review identifies key limitations in existing approaches, such as poor adaptability to dynamic threat landscapes, the absence of lightweight yet effective protection techniques, and inadequate implementation of end-to-end security frameworks. Addressing these gaps, the research formulates a problem statement centered on improving IoT network security through a scalable and efficient methodology.A comprehensive system architecture and methodological framework are proposed to mitigate identified vulnerabilities while maintaining compatibility with the resource constraints of IoT devices. The proposed solution is evaluated against existing techniques, focusing on detection accuracy, computational efficiency, and overall security enhancement. Comparative analysis shows that the approach delivers a more effective defense mechanism for IoT environments, emphasizing the need for advanced, adaptive, and practical security frameworks for future IoT deployments.

KEYWORDS: IoT Security, Emerging Threats, Network Vulnerabilities, Security Framework.

1. INTRODUCTION

Internet of things (IoT) is a group of interconnected devices and people in which devices can communicate with each other without human intervention [1].

The internet of things allows people and things to be connected anytime, anyplace with anything and anyone, ideally using any path/network and any service.

The ultimate objective of IoT is to create "A better World for human beings".

2. SECURITY ISSUE FOR IOT

Why Security???

- As these large numbers of devices directly associated with the open web; they provides a " Fertile ground" for launching different security threats with in the network.
- Intruders can compromise the data security as well as privacy because of that.
- If the Security will be compromised, then there will be no any potential benefits of this upcoming emerging technology to the Society in any domain like Healthcare, Agriculture or Smart City.
- IoT is a Resource constrained network. So, traditional approaches of security can not be deployed with in the IoT network. So, to develop a lightweight and efficient approach for IoT Security is prime research direction in current time.

Research Paper

Attacks Threat Model for IOT

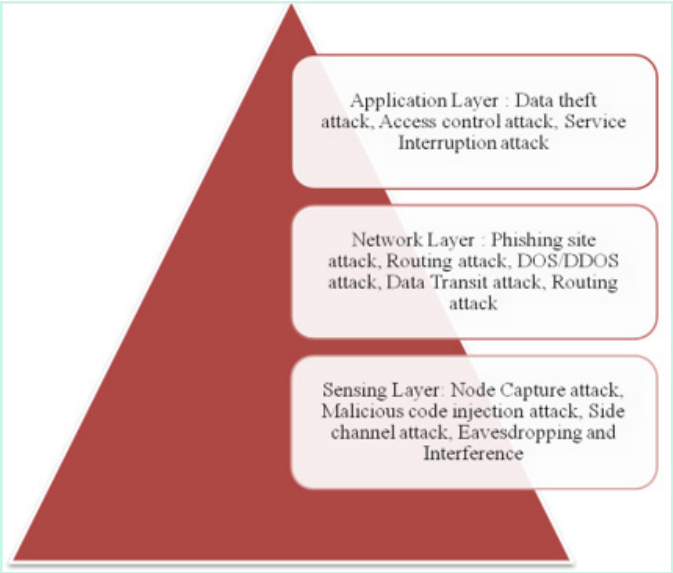

Fig. 1: IOT Threat Model

3. ATTACKS ON IOT [12]

- Physical Attacks: These kinds of attacks are focused on the hardware components of the IOT system and the attacker needs to be physically close or into the IOT system in order to make the attacks working. Some examples of these attacks are:
- (1) Node Tampering
- (2) Malicious code injection attack
- Impersonation Attack: Authentication in the distributed environment is very difficult, allowing malicious nodes to use a fake identity for malicious attacks.
- Denial of Service Attack: An attacker floods the network with large traffic so that services/ resources are unavailable to its intended(legal) users.
- Distributed Denial of Service Attack: DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.
- Routing Attacks: Intermediate malicious nodes might modify the right routing paths during the data collection and forwarding process.
- Data Transit Attacks: various attacks on the confidentiality and integrity during data transit in access or core networks. Some of types of Data Transit attacks are:

a. Man-in-the-Middle attack
b. Traffic Analysis attack
c. Modification attack
d. Replay attack

3.1 IOT Security Services

- Authentication : The process of confirming and insuring the identity of objects.
- Authorization : The process of giving permission to an entity to do or have something.
- Integrity : The way toward keeping up the consistency, precision and dependability of information over its whole life cycle.
- Confidentiality: The process of ensuring that the information is only accessed by authorized people.
- Availability: The process of ensuring that the service needed is available anywhere and anytime for the intended users.
- Privacy: The process of ensuring non-accessibility to private information by public or malicious objects.

Fig. 2: IOT Security Services

4. WHY AUTHENTICATION???

- Authentication is the way of identifying users/ devices unambiguously in a network and based on that granting access to the legal users/devices.
- It is one of way to prevent from various common attacks such as Replay attack, MITM attack, Impersonation attack etc…
- If there is no authentication algorithm properly implemented in network then important credentials can be stolen by attacker and it can harm to the network or user.
- So, Authentication is one of the important

security element for IOT network based on which various devices can do communication with each other and can share the data with trust. Based on Authentication; Validity of device/user can be done in network.

5. COMPARISON OF EXISTING AUTHENTICATION APPROACHES FOR IOT

Table 1: Comparison of Existing Authentication approaches for IOT

Identity based Authentication	Token based Authentication	PUF based Authentication	Context based Authentication	Procedure based Authentication
Shared secret key , password	A piece of data-Token	Hardware based approach, IC circuit mounted on chip based on Challenge – Response pair.	Physical context or Behavioural context.	One-way Authentication or Mutual Authentication
Important credentials are stored at internal memory of device	Tokens will be issued by Authorization server (AS) for accessing resource.	device will compute response based on PUF and will provide it to server.	Context information like location, radio signal features will be verified for authentication.	No Cryptographic assets will be stored in memory. Challenge will be provided by server,
Key Stolen attack, Password leakage attack, Side channel attack, location spoofing attack is possible.	Replay attack, Man in the Middle attack, Impersonate attack, DOS attack is possible.	Modelling attack, Man in the Middle attack is possible.	Modification attack, Interception attack is possible.	Although no cryptographic data is kept in memory and challenges are server-issued, risks such as key extraction, credential leakage, side-channel exploits, and location spoofing can still occur.

6. LITERATURE REVIEW

Table 2: Literature Review

Sr. No.	Title	Journal & Year	Main Idea/Contribution	Layer on which Paper Focuses
1.	Secure Two-Factor Authentication for IoT Device	IEEE , 2022	The authors design a secure mutual two-factor authentication protocol combining: (1) RFID token (something you have) (2) Fingerprint biometric (something you are) The system includes two phases: (1) Registration: enrolling RFID and fingerprint data. (2) Authentication: verifying both credentials against stored templates.	Perception Layer Uses RFID & fingerprint at device level
2.	Designing a Lightweight IoT Authentication Protocol for Resource-Constrained Devices	IEEE , 2024	A lightweight mutual authentication protocol using Elliptic Curve Cryptography (ECC) to leverage low computational and communication costs. Four protocol phases: • Initialization • Device setup • Authentication • Password-change support, which is not common in many existing schemes	This protocol addresses two primary layers of the IoT architecture: -Perception Layer Directly involves resource-constrained IoT devices—like sensors or RFID tags that perform registration and authentication locally using ECC primitives -Network Layer: the protocol covers message exchange, nonce-based session handshakes, and secure communication

3.	LPA: A Lightweight PUF-based Authentication Protocol for IoT System	IEEE , 2023	• Introduces LPA, a lightweight mutual authentication and key-exchange protocol for IoT devices using Physical Unclonable Functions (PUFs) • Utilizes PUF challenge-response behavior along with lightweight operations (e.g., XOR, hashing) for authentication and session key generation.	LPA spans the following layers of the IoT architecture: -Perception Layer: PUF-enabled devices conduct authentication locally. -Network Layer: Key exchange and message coordination with a centralized trust server. It does not extend to Edge/Fog or Application layer concerns.
4.	IoT Authentication Protocols: Classification, Trend and Opportunities	IEEE Transactions on Sustainable Computing, 2025	• This comprehensive survey explores three key dimensions of IoT authentication protocols: • Classification and limitations of existing schemes • Emerging trends and innovation in the field • Opportunities and future directions for researchers and practitioners • Auth Categories: ECC-based, hash/symmetric, PUF, blockchain, ML/behavioral, multi-factor • Trends: Blockchain, ML-fueled continuous auth, zero trust, biometric UX, Lightweight Cryptography	
5.	PUF-Based Mutual Authentication and Key Exchange Protocol for Peer-to-Peer IoT Applications	IEEE Transactions on Dependable and Secure Computing, 2023	Each IoT endpoint is equipped with a Physical Unclonable Function (PUF) to generate device-specific secrets on the fly, eliminating stored keys or challenge-response pairs (CRPs) on the device or central database Uses lightweight operations: PUF responses, hashing, and XOR. Enables mutual authentication and session key establishment directly between two peer devices in a decentralized fashion	-Perception Layer: PUF-equipped endpoints performing local authentication -Network Layer: Direct P2P message exchange and session establishment
6.	An Improved Lightweight Two-Factor Authentication Protocol for IoT Applications	IEEE Transactions on Industrial Informatics, 2023	The enhanced scheme combines Physical Unclonable Functions (PUFs) with wireless link fingerprints Two factors used: PUF-derived hardware fingerprint, eliminating stored keys or CRPs. Wireless fingerprint derived from radio link characteristics between device and gateway or server. Covers registration, mutual authentication, key agreement, and secure data transfer phases using lightweight primitives like XOR and secure hash functions	Perception Layer: PUF-equipped IoT devices and wireless fingerprint sensing Network Layer: Secure message exchanges and challenge response handshakes with the gateway

Sr No.	Title	layer	Key- stolen Attack	Impersonation Attack	**Replay Attack**	**DOS Attack**	**Interception Attack**	**MITM Attack**	**Modeling attack**	**Spoofing Attack**	**Physical attack**
1	[1]	A	N	N	N	Y	Y	N	N/A	N	N
2	[2]	A	N	Y	Y	N	N	N	N/A	N	N
3	[3]	P	N/A	Y	N	N	N	N	N/A	Y	N
4	[4]	A	Y	N	N	Y	N	Y	N	N	N
5	[5]	A	Y	Y	N	N	N	N	Y	N	N
6	[6]	A+P	Y	Y	N	N	N	N	N	Y	N

7	[7]	A	N	Y	Y	N	N	N	N/A	N	N
8	[8]	A	N	Y	Y	N	N	Y	N/A	N	N
9	[9]	P	Y	Y	N	N	Y	N	N/A	N	N
10	[10]	A	N/A	Y	N	N	N	N	N/A	N	N
11	[11]	A+P	Y	Y	N	N	N	N	N	Y	N
12	[12]	P	Y	Y	N/A	Y	N	N	N	Y	N

Where; A= Application Layer, N= Network Layer and P= Physical Layer

Y indicates particular attack is addressed in given research article and N represents suggested approach may leads to particular attack.

7. SURVEY CONCLUSION

- Internet of Things (IoT) is a group of interconnected devices & peoples in which device can communicate with each other without human intervention.
- In this presentation ; we have provided fundamental information about IoT including definition , architecture & security challenges faced by IoT systems. We have briefly described IoT Threat Model also. Then we have presented related research work which already has done in Authentication domain for securing IoT devices / system.

8. RESEARCH GAP

(1) Most of the existing Authentication methods for IOT network use a single key based approach / password based approach to authenticate IOT device. From the literature survey we found that such kinds of the methods are vulnerable to the different attacks such as Key stolen attack, Side channel attack, MITM attack, Device cloning attack. If the password also not changed over the time, then also it is prone to Dictionary attack. And if the adversary has the shared key/password, an identical fake device also can be made.

So, there is a need to work on authentication approach in which key value should be changed over the time. So, if adversary gets shared key than also he/she can not get access of the system and can not compromise with system security.

We can provide security against MITM attack, Interception attack, Dictionary attack, Key stolen attack, Device cloning attack and Replay attack.

(2) IOT devices are deployed in open and public places, which may cause them to be vulnerable to various Physical and cloning attack. So, it is important that any security solution designed for IOT devices should not only be efficient but also can detect any violations of physical security of IOT devices.

This kind of authentication technique sometimes leads to the ambiguous device identification in which device identity is only verified but the context information of device is not taking into consideration. It may leads to various Physical attack, changing distance attack and location spoofing attack.

One approach to solve this problem is the integration of information about the physical context of a device to improve the authentication process.

9. PROBLEM STATEMENT

The majority of existing Authentication methods for IoT are Key based/ Password based methods. Existing Key based authentication algorithms are vulnerable for Key stolen, Dictionary attack, MITM attack & Replay attack. So, for providing better security in IOT Network; multi-key based authentication approach is needed.

10. ADVANTAGE OF DYNAMIC KEY BASED IOT AUTHENTICATION [22, 23, 25, 28]

However, in symmetric encryption, both sides of communication share the same pair of keys. Once the key is known by the third party, or the third party just analyzes the network traffic, the communication content will be inferred. Therefore, the long-term use of a fixed session key is insecure among IoT devices.

Need for “One time One Cipher”: Every time the key used for encryption and decryption will differ and expire after each session. This ensures the uniqueness and dynamic nature of the key.

11. METHODOLOGY

Dynamic Key Authentication

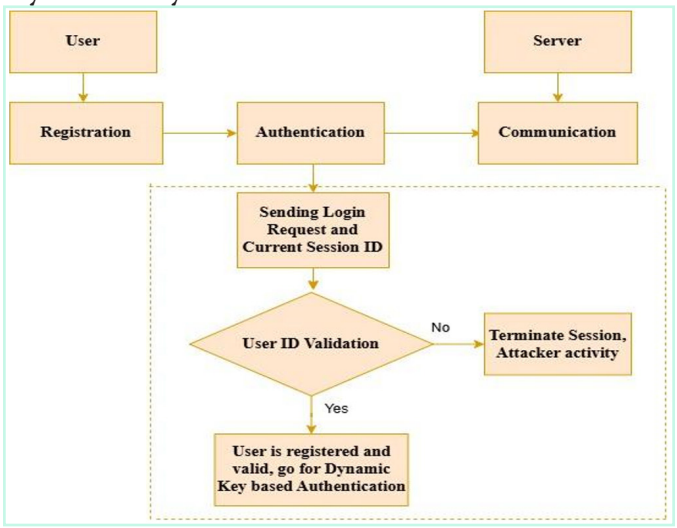

Fig. 3: Dynamic Key Authentication

12. ALGORITHM STRUCTURE

Fig. 4: Proposed Authentication Algorithm Structure

Registration Phase:

All the client IoT devices have to register with the server, a client IoT device Ci generates a registration request with IDi and sends this registration request to the Server.

When Server receives a registration request of any client IoT device; Server will make entry of that client device into its database.

Registration Request : {Device ID, Device Password}

Mutual Authentication & Session Key Establishment

IoT device and Server will mutually authenticate to each other. And after successful authentication; they will establish session key for further communication.

Concept of Dynamic key based authentication for Mutual Authentication & Session Key Establishment phase.

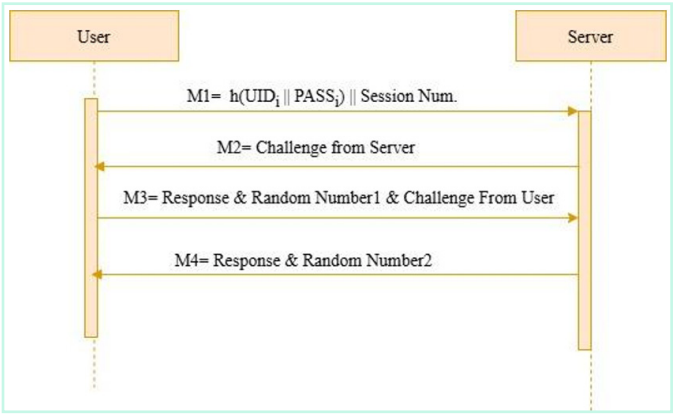

Fig. 5: Proposed Authentication Algorithm Structure

12.1 Dynamic Key Based Authentication

Table 3: Existing Approaches for Dynamic Key Generation for IoT Authentication [22, 23, 25, 28]

Notation	Description
||	Concentation Operation
$\oplus$	Ex-OR Operation
h	Message Digest Function
Random Number	64 bit Random Number for Mutually Authentication Purpose
Temporary Number (Nonce)	64 bit Random Number for Session Key Generation Purpose

Vault: The Vault contains 64 keys each key 64 bits long in hexadecimal format. All these keys will be stored into 8*8 Matrix form at the IoT Device side and Server side. At the Device side and Server side it can be stored in encrypted mode for security purpose. This 8*8 matrix will be shared between IoT device and Server during initial deployment time.

Table 4: Sample validation

	1	2	3	4	5	6	7	8
1	112f	3a4e	56bf	76ed	4eda	2bcf	8a0c	10bc
2	45cd	54f3	12ab	Cd52	Ab27	35ed	9a4c	1f9c
3	32ab	2e3d	1f22	2c3d	44ab	234c	1d5f	445c
4	Cf12	Def3	12ae	16cd	24af	26cd	1c7f	2d8f
5	24ab	3ea4	1f26	2c3a	4c3d	23ce	1d5a	4e5c
6	9f12	7ef3	19ae	46cd	29af	22ce	1a7c	2a8b
7	211c	3b4e	67bf	87ed	47da	21cf	810c	19bc
8	42ca	45f3	24ab	2252	152b	359d	9a4d	1f9a

IoT Device will initiate the communication request to IoT Server. Request message M1 contains the message digest of Device ID and Session number to

maintain the authentication session.

$$M1 = h\ (Device\ ID \| Device\ Password) \| Session\ Number$$

Server will verify message digest value for device id and if it is valid, then Server will generate Challenge Message M2 for IoT Device.

M2 contains a Challenge1 and Random number1. Challenge consists of q distinct numbers and each number will points towards index of a 8*8 Matrix, stored in a vault. The value of q should be less than total number of keys stored in a vault

$$Challenge_1 = \{C1, C_2, C_3, \dots, C_8\}.$$

$$M2 = \{Challenge_1, Random\ Number_1\}$$

IoT Device generates the response for the assigned challenge. IoT device generates a temporary key of 64 bits from the Vault by performing XOR operation on all the key values whose index are present in the challenge message.

$$Temporary\ Key\ K1\ at\ IoT\ Device\ Side = K[C_1] \oplus K[C_2] \oplus \dots \oplus K[C_q].$$

IoT device generates response by performing encryption of Random Number1 || Temporary Number1 by using K1 as a encryption key.

Here, Temporary Number1 (Nonce) is a 64 bit number generated by IoT device randomly for future use to generate Session key for further communication.

$$M3 = Enc\ (K1, Random\ Number_1 \| Temporary\ Number\ (Nonce)_1 \| \{ Challenge_2, Random\ Number_2 \}).$$

IoT device also generates a separate challenge message for IoT server using the same method. IoT device now send generated response for the Server's challenge and Challenge for server.

$$Challenge2 = \{C1, C2, C3, \dots, C8\}.$$
(It should be different from Challenge1 Values).

After receiving message from the device, Server will generate temporary key by using indexes of Challenge2from its secure vault. There is no need to share key here between IoT device and Server.

After generating key K1, Server will decrypt the message M3. If the server retrieves the Random number1 from the M3 message, it signifies that receiver of previous challenge message M2 was legal IoT Device. And after that, Server will generate response for Client IoT Device's challenge M3.

$$Temporary\ Key\ K2\ at\ Server\ Side = K[C_1] \oplus K[C_2] \oplus \dots \oplus K[C_q].$$

$$M4 = Enc\ (K2, Random\ Number_2 \| Temporary\ Number\ (Nonce)_2).$$

The IoT Device will receive message M4 and decrypts it by generating temporary key K2 from its secure vault by utilizing content of Challenge C2. And if IoT device gets back Random number2 then Server is also authenticated.

After IoT Device and Server mutually authenticate each other, they will generate temporary session key by using Temporary Number1 and Temporary Number2.

$$Session\ Key = Temporary\ Number_1 \oplus Temporary\ Number_2$$

[3] Session Key Modification Phase:
Dynamic Session Key
After expiration of session time period; Server will challenge the client and Client will challenge the Server for mutual authentication purpose and then they will mutually establish new session key.

13. CONCLUSION

The analysis of existing IoT authentication mechanisms reveals that traditional key-based and password-based approaches remain highly vulnerable to key theft, dictionary attacks, replay attacks, and man-in-the-middle attempts. Although several dynamic key-generation techniques exist, most rely on predictable device-specific physical properties or linear structures such as LFSRs, which significantly limits their security strength. Therefore, the need for a robust authentication framework in IoT networks is

evident. A multi-key–based authentication strategy that follows the "one-time, one-cipher" principle—where multiple independently generated keys are refreshed for every session—offers a promising direction. Such dynamic, time-varying key generation can greatly enhance resistance to cryptographic attacks, strengthen session confidentiality, and provide a more secure foundation for resource-constrained IoT environments

REFERENCES

1. I. Cetintav and M. Tahir Sandikkaya, "A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs," in IEEE Access, vol. 13, pp. 37703-37723, 2025, doi: 10.1109/ACCESS.2025.3546147.
2. A. Sharma, R. Suganya, P. B. Krishna, R. Raj and R. Kumar Murugesan, "Network Efficient Hierarchical Authentication Algorithm for Secure Communication in IoT and IoE," in IEEE Access, vol. 12, pp. 195926-195942, 2024, doi: 10.1109/ACCESS.2024.3516886.
3. Zhao, J.; Hu, H.; Huang, F.; Guo, Y.; Liao, L. Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. Electronics 2023, 12, 1812. https://doi.org/10.3390/electronics12081812
4. M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov and M. Derawi, "A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 101362-101384, 2022, doi: 10.1109/ACCESS.2022.3207472.
5. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
6. Y. Lee, J. Yoon, J. Choi and E. Hwang, "A Novel Cross-Layer Authentication Protocol for the Internet of Things," in IEEE Access, vol. 8, pp. 196135-196150, 2020, doi: 10.1109/ACCESS.2020.3033562.
7. Z. Liu, C. Guo and B. Wang, "A Physically Secure, Lightweight Three-Factor and Anonymous User Authentication Protocol for IoT," in IEEE Access, vol. 8, pp. 195914-195928, 2020, doi: 10.1109/ACCESS.2020.3034219
8. N. Wang, T. Jiang, S. Lv and L. Xiao, "Physical-Layer Authentication Based on Extreme Learning Machine," in IEEE Communications Letters, vol. 21, no. 7, pp. 1557-1560, July 2020, doi: 10.1109/LCOMM.2017.2690437. .
9. N. M. Karie, N. M. Sahri and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), Sydney, NSW, Australia, 2020, pp. 22-29, doi: 10.1109/ETSecIoT50046.2020.00009.
10. Jeffry Voas, Bill Agersti " A Closer look at the IOT's Things" published at IT Professional Vol. 20, Issue 3, May-2018.
11. M. Mehta, H. Baldaniya and N. Goriya, "A Systematic Review of Authentication Methods for Internet of Things," 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp. 1-6, doi: 10.1109/INOCON50539.2020.9298304.
12. El-hajj, Mohammed, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni, "A Survey of Internet of Things (IoT) Authentication Schemes" Sensors 19, no. 5: 1141. https://doi.org/10.3390/s19051141
13. R. R. Pahlevi, V. Suryani, H. H. Nuha and R. Yasirandi, "Secure Two-Factor Authentication for IoT Device," 2022 10th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 2022, pp. 407-412, doi: 10.1109/ICoICT55009.2022.9914866.
14. V. K. Rai, S. Tripathy and J. Mathew, "LPA: A Lightweight PUF-based Authentication Protocol for IoT System," 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom, 2023, pp. 1712-1717, doi: 10.1109/TrustCom60117.2023.00233.
15. A. N. Alsheavi et al., "IoT Authentication Protocols: Classification, Trend and Opportunities," in IEEE Transactions on Sustainable Computing, vol. 10, no. 3, pp. 515-533, May-June 2025, doi: 10.1109/TSUSC.2024.3492152.
16. Y. Zheng, W. Liu, C. Gu and C. -H. Chang, "PUF-Based Mutual Authentication and Key Exchange Protocol for Peer-to-Peer IoT Applications," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 3299-3316, 1 July-Aug. 2023, doi: 10.1109/TDSC.2022.3193570.
17. A. M. A. Modarres and G. Sarbishaei, "An Improved Lightweight Two-Factor Authentication Protocol for IoT Applications," in IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 6588-6598, May 2023, doi: 10.1109/TII.2022.3201971.
18. D. He, Y. Cai, S. Zhu, Z. Zhao, S. Chan and M. Guizani, "A Lightweight Authentication and Key Exchange Protocol With Anonymity for IoT," in IEEE Transactions on Wireless Communications, vol. 22, no. 11, pp. 7862-7872, Nov. 2023, doi: 10.1109/TWC.2023.3257028.
19. Lin Wang, Honan An et al. "Security Enhancement on a Lightweight Authentication Schema with Anonymity Fog Computing Architecture", IEEE Access, Vol.8, pp. 97267-97278, May-2020.
20. Jason M. Mcginthy, Alan J. Michaels "Further Analysis of PRNG- Based Key Derivation Functions", IEEE Access, Vol.7, pp. 95978-95986, July-2019.
21. E.Barker, NIST Special Publication, document 800-857, 2016.
22. Yuwen Chen, Joes-Fernam et al. " A Lightweight Anonymous Client- Server Authentication Scheme for the Internet of Things Scenario: LAuth", Sensors, 2018, 18, 3695.
23. Lukas Nemec, Vashek Matyas et al. "Evaluating Dynamic Approaches to Key (Re-) Establishment in Wireless Sensor Networks", Sensors, 2019, 19, 914
24. Ana Reyna, Cristian Martin et al. "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems 88, Elseveir, pp. 173-190, 2018.
25. Jing Tian, Gang Xiong et al. "A Survey of Key Technologies

for Constructing Network Covert Channel", Security and Communication Networks, vol. 2020, Hindawai.
26. Shiju Sathyadevan, Krishnashree Achuthan et al. "Protean Authentication Scheme- A Time-Bound Dynamic KeyGen Authentication Technique for IOT Edge Nodes in Outdoor Deployments", IEEE Access, Vol. 7, pp. 92419-92435, 2019.
27. Khawaja Mansoor, Anwar Ghani et al. "Securing IOT-Based RFID Systems: A Robust Authentication Protocol Using Symmetric Cryptography", Sensors, 2019, 19, 4752.
28. Daniel A.F. Saraiva, Valderi Reis et al. "PRISEC: Comparision of Symmetric Key Algorithms for IOT Devices", Sensors, 2019, 19, 4312.
29. Mario Frustaci, Pasquale Pace et al. "Evaluating Critical security issues of the IOT world: Present and Future challenges", IEEE Internet of Things Journal, 2017.
30. https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php