RT&A, No 4 (89)
Volume 20, December 2025

AUTHENTICATION APPROACHES IN IOT: A COMPARATIVE STUDY OF EXISTING METHODS AND FUTURE DIRECTIONS

Dr. Mihir Mehta[1], Dr.Sanjay Patel[2], Nrupesh Shah[3]

•

[1]Assistant Professor, Computer Engineering department, G.E.C., Gandhinagar, India.
mihir_mehta@gecg28.ac.in
[2] Associate Professor, Computer Engineering department,G.E.C., Gandhinagar, India.
sppatel@gecg28.ac.in
[3]Assistant Professor, Computer Engineering department, G.E.C., Gandhinagar, India.
nrupesh_shah@gecg28.ac.in

Abstract

The Internet of Things (IoT) marks a new era in how humans interact with technology. It enables physical devices to generate, receive, and effortlessly exchange data with each other. The primary objective of IoT-based systems is to enhance user convenience and operational efficiency. However, IoT environments are typically open and interconnected, which exposes them to a wide range of security threats. Ensuring robust security is therefore a critical aspect of IoT networks. Traditional security mechanisms are often unsuitable due to the limited computational resources of IoT devices. Authentication plays a key role in verifying the identity of each device within the network, as compromised devices can significantly disrupt operations. To fully leverage IoT's potential, it is crucial to address and resolve security concerns across all layers. The research is divided into two primary categories: authentication factors and widely used cryptographic primitives. Authentication factors encompass methods like passwords, RFID, smart cards, and one-time passwords (OTPs), whereas cryptographic primitives involve techniques such as Data Encryption Standards (DES), Advance Encryption Standard (AES) and Physically Unclonable Functions (PUFs). This paper reviews existing authentication techniques and provides the comparison among them. Our research works also highlights the performance of various cryptographic techniques in IoT network. Reliability denotes the consistent and accurate functioning of an authentication system in verifying that only authorized devices and users are granted access to the IoT network or its associated services.Reliable Authentication framework offers consistent Identity verification & minimizes False Positive- Unauthorized devices mistakenly authenticated/ False Negatives- Legitimate devices wrongly denied access. It concludes with identification of various open research challenges associated with IoT Authentication.

Keywords: IoT, Authentication, Encryption, PUF, OTP, Smart Card, Multi-factor Authentication

I. Introduction

The Internet of Things (IoT) is an ecosystem of interconnected objects and individuals, enabling smart communication with minimal human intervention. IoT facilitates connectivity between people and devices anytime, anywhere, using any platform or service [14]. Its overarching goal is to build a smarter world where devices understand users' preferences, needs, and behaviors, and

DOI: https://doi.org/10.24412/1932-2321-2025-489-716-730

respond automatically without explicit commands [15]. The Internet of Things (IoT) refers to the expanding network of intelligent physical devices—such as smart phones, wearable, home appliances, smart farming systems, smart grids, smart waste management, smart homes, smart cities, smart transportation, industrial equipment, and medical devices—that can sense their surroundings, process information, and interact with other connected systems. These devices are capable of collecting and exchanging data to support automation and decision-making.

As the use of IoT applications continues to rise, the number of connected devices is also growing, resulting in an increased volume of data traffic across networks [25]. According to Cisco, over 500 billion devices are expected to be connected to the Internet by the end of 2025. Similarly, a 2015 report by the McKinsey Global Institute estimated that the IoT could contribute between $3.9 trillion and $11.1 trillion annually to the global economy by 2025[25].The main goal of IoT is to transform everyday life and work by offering intelligent tools and automated services that simplify daily tasks. However, despite significant advancements and growing adoption, several challenges still hinder the full and effective deployment of IoT in real-world environments.

Among these challenges, security stands out as a critical concern. IoT systems are increasingly exposed to a wide range of security threats, which are becoming more complex and prevalent [7], [8]. Research has identified various vulnerabilities in IoT environments, including issues related to authentication, authorization, confidentiality, and different types of cyber-attacks [7], [9], [10]. As a result, IoT security has become a major focus area for researchers, industries, and the public, demanding further in-depth investigation and innovative solutions.

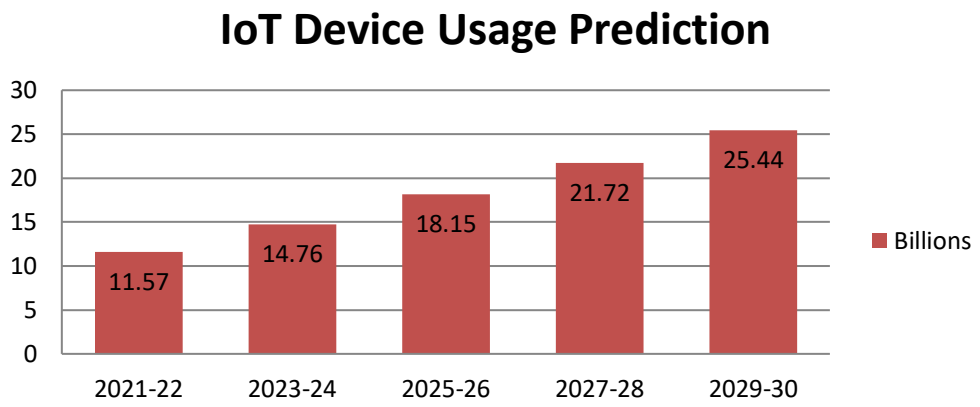

Figure 1: *IoT Device Usage Prediction [25]*

The IoT architecture consists of several core elements: sensors, aggregators, communication channels, external utilities, and decision triggers.

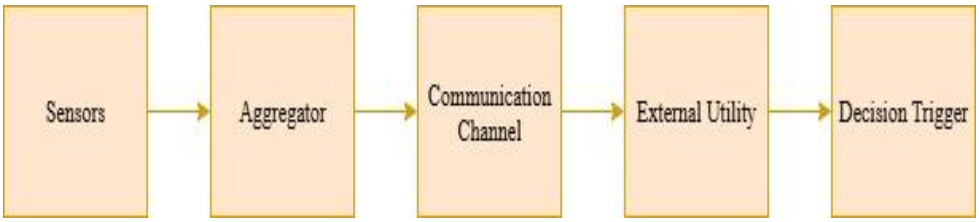

Figure 2: *Components of IoT [2]*

Sensors are electronic components that detect physical attributes like temperature, motion, pressure, sound, proximity, or identity. All sensors utilize mechanical, electrical, chemical, optical, or other forms of interaction at the interface between a controlled process and the surrounding environment.

Aggregators handle data collection and management. An aggregator is a software-based solution that applies a mathematical function to convert raw data into intermediate, summarized data—commonly used for handling and analyzing large volumes of data.

Communication channels serve as pathways for data transmission. A communication channel facilitates the transfer of data among computing, sensing, and actuation components. The flow of data through the channel can be either one-way or two-way.

External utilities refer to third-party hardware or software resources such as cloud services, mobile phones, and databases. Lastly, decision triggers generate actionable outcomes based on predefined objectives and contextual inputs from the system [17].

Decision triggers are typically implemented virtually through code, as they represent conditional expressions that initiate specific actions. They abstractly define the ultimate goal of an Internet of Things (IoT). While many can be understood as "if-then" rules, not all follow this exact format.

I.Architecture of Internet of Things

The IoT architecture is typically structured into three main layers: the Perception Layer, the Network Layer, and the Application Layer [16].

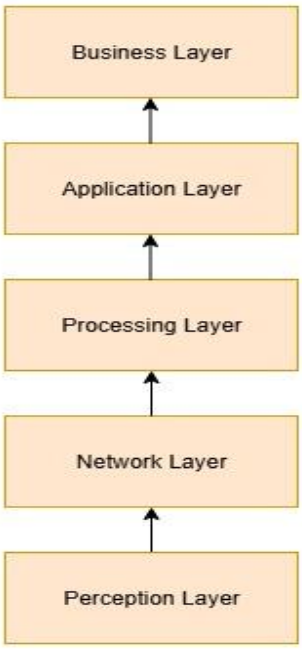

Figure 3: *IoT Architecture [16]*

1. **Perception Layer**: This layer facilitates connectivity among a variety of devices, including physical components like sensors, Radio Frequency Identification (RFID), and Bluetooth, along with virtual elements such as barcodes, Quick Response (QR) codes, and Global Positioning System (GPS). Its main role is to gather data from end nodes and forward it to

the network layer. The devices operating within this layer are generally recognized as resource-constrained. [16].

2. **Network Layer**: Positioned between the perception and Processing layers, the network layer—also known as the transmission layer—handles the reliable and fast delivery of data collected by the perception layer to the application layer [16]. This layer handles the collection of data sent by the end nodes in the perception layer and ensures its delivery to the application layer. Its primary function is to maintain connectivity with the devices within the perception layer, utilizing technologies like 4G and Wi-Fi.
3. **Processing Layer**: Positioned between Network and Application layer- responsible for processing & storage of collected data from the network layer. It also provides facility for the analysis of collected data. It uses various cloud services for the data storage & ML Models for the data analysis purpose [16].
4. **Application Layer**: This layer is responsible for delivering specific services and functionality to end users. For instance, it may provide users with data such as temperature readings or humidity levels, depending on the needs of the application [16].
5. **Business Layer**: This is the top most layer of IoT Architecture. It is responsible for managing business operations & overall strategies of business. It ensures alignment between IoT services and Organizational goals [16]. The components of business layers are decision making systems, revenue models, policy & regulation policies of the organization.

II. Security Challenges for IoT

1. **Open Architecture**: IoT devices are directly connected to the internet, which is inherently open and public. This openness significantly increases the risk of various types of cyber-attacks [18].
2. **Resource Constraints**: IoT devices typically have limited storage capacity, computing power, and battery life. These limitations make it difficult to apply conventional security algorithms, which are often too heavy for such environments [18].
3. **Lack of Standardization**: IoT devices vary widely in terms of hardware, firmware, and communication interfaces. This heterogeneity makes it difficult to establish universal security standards. Although it's crucial to design secure code and perform rigorous testing during manufacturing, implementing consistent security mechanisms across all devices remains a challenge [18].
4. **Trust and Data Integrity Issues**: With a large number of devices connected to the internet, it becomes nearly impossible to ensure that each one is adequately protected and regularly updated. A single compromised device can potentially jeopardize the entire network. Therefore, establishing trust and verifying data integrity at the device level is critically important [18].
5. **Software Vulnerabilities**: Given the scale of connected devices, ensuring that every device is secure and updated with the latest patches is unrealistic. A single weak link can provide unauthorized access to thousands of devices. As a result, verifying the reliability and authenticity of software running on each device is essential [18].

III. Key Security Issues in IoT

1. **Authentication:** This is the process of verifying the identity of devices or users in an IoT system and granting access only to authorized entities. Authentication mechanisms help mitigate threats like man-in-the-middle (MITM) attacks, replay attacks, and impersonation

attempts. Research indicates that authentication is currently among the most trusted and widely used techniques to control access in IoT networks. Various authentication methods include:Identity-Based Authentication, Token-Based Authentication, PUF (Physical Unclonable Function)-Based Authentication, Procedure-Based Authentication, etc.and Each method offers distinct advantages and limitations.

2. **Encryption:** To ensure end-to-end security in communication, encryption is vital. It protects the confidentiality of data during transmission using either symmetric or asymmetric cryptographic algorithms. However, conventional encryption methods like AES and DES are often too demanding for IoT devices due to their constrained processing capabilities. Therefore, encryption algorithms for IoT must be lightweight and energy-efficient.
3. **Trust Management:** Trust mechanisms help identify and isolate malicious devices in the network. Trust-based access control systems evaluate the behavior of each node and compute trust scores dynamically. However, this approach demands significant computational resources, which can be a challenge in energy-limited IoT environments.
4. **Secure Routing:** Malicious nodes can disrupt IoT communications by redirecting data packets through unauthorized routes. Such nodes may participate in routing decisions and launch various routing-based attacks, including:Sinkhole Attacks, Wormhole Attacks, Sybil Attacks, etc.

IV. Importance of Authentication in IoT

Authentication plays a crucial role in clearly identifying devices and users in a network and granting access solely to authorized entities. It serves as a first line of defense against many common security threats such as replay attacks, man-in-the-middle (MITM) attacks, and impersonation attempts [20].

By authenticating users and devices, IoT systems can ensure that data being sent or received hasn't been tampered with and is coming from a verified source. This helps preserve the integrity and confidentiality of sensitive information. Strong authentication mechanisms help detect and prevent attempts to clone or manipulate IoT devices, which is crucial for physical and operational security.

Without proper authentication mechanisms, attackers can intercept confidential credentials, compromise network integrity, and gain unauthorized access, potentially leading to serious disruptions. Thus, authentication is a fundamental requirement for secure communication in IoT systems.

It builds a foundation of trust by verifying the legitimacy of each entity attempting to interact within the network. A robust authentication system ensures that only verified devices and users are permitted to exchange data, thereby maintaining the security and reliability of IoT applications.

If a device's identity is falsified or compromised, it can expose the entire network to a variety of attacks, including masquerading, denial-of-service (DoS), and data tampering. Given these risks, authentication has emerged as a widely adopted security technique in IoT ecosystems to maintain device integrity, restrict unauthorized access, and support secure interactions among connected devices [19].

II. Literature Review

I. Comparison of Existing Authentication approaches in IoT

Several authentication mechanisms have been developed for IoT systems, each offering varying levels of security and efficiency.

1. **Identity-Based Authentication** is straightforward to implement and requires storing certain credentials within the device's memory. Identity-based authentication schemes utilize one (or a combination) of hash, symmetric or asymmetric cryptographic algorithms. However, this stored data can become a security risk, making the system vulnerable to key theft, side-channel attacks, and similar threats.
2. **Token-Based Authentication** provides an alternative that avoids storing permanent credentials on the device. Instead, devices use access tokens issued by an authorization server. This method helps mitigate key theft but still leaves the system exposed to token capture and replay attacks.
3. **Physical Unclonable Function (PUF)**-based Authentication is a hardware-level method that leverages unique physical properties of a device for identification. It does not require storing secrets in memory, making it more resistant to key extraction and memory attacks. Authentication is achieved using challenge-response pairs generated by the physical characteristics of the hardware. A Physical Unclonable Function (PUF) functions through a challenge-response system, where the device's inherent physical attributes act as the challenge, and the corresponding digital output serves as the response. This interaction produces a distinct identifier unique to each device. Due to the non-replicable nature of these physical traits, PUFs offer a strong level of security [24].
4. **Context-Based Authentication** can be layered onto any of the above methods to enhance security further. By including contextual elements like location, time, or usage behaviour, authentication becomes more robust and harder to bypass or forge. This combination can significantly strengthen authentication mechanisms for IoT devices operating in open and vulnerable environments. Context information can be Physical or Behavioural. Physical**:** Biometrics derived from an individual's physical traits, such as fingerprints, hand geometry, retinal scans, and similar features. Behavioural**:** Biometrics based on an individual's behaviour patterns, including keystroke dynamics (the rhythm and timing of typing), gait analysis (the study of walking or running patterns), and voice identification (authentication using unique voice prints).
5. **Authentication Procedure:** One-way authentication: In this method, when two parties intend to communicate, only one of them verifies its identity to the other, while the second party does not provide any authentication. Two-way authentication: Also known as mutual authentication, this approach involves both parties verifying each other's identities. Three-way authentication: In this model, a trusted central authority is involved to authenticate both parties and assist them in verifying each other's identities.

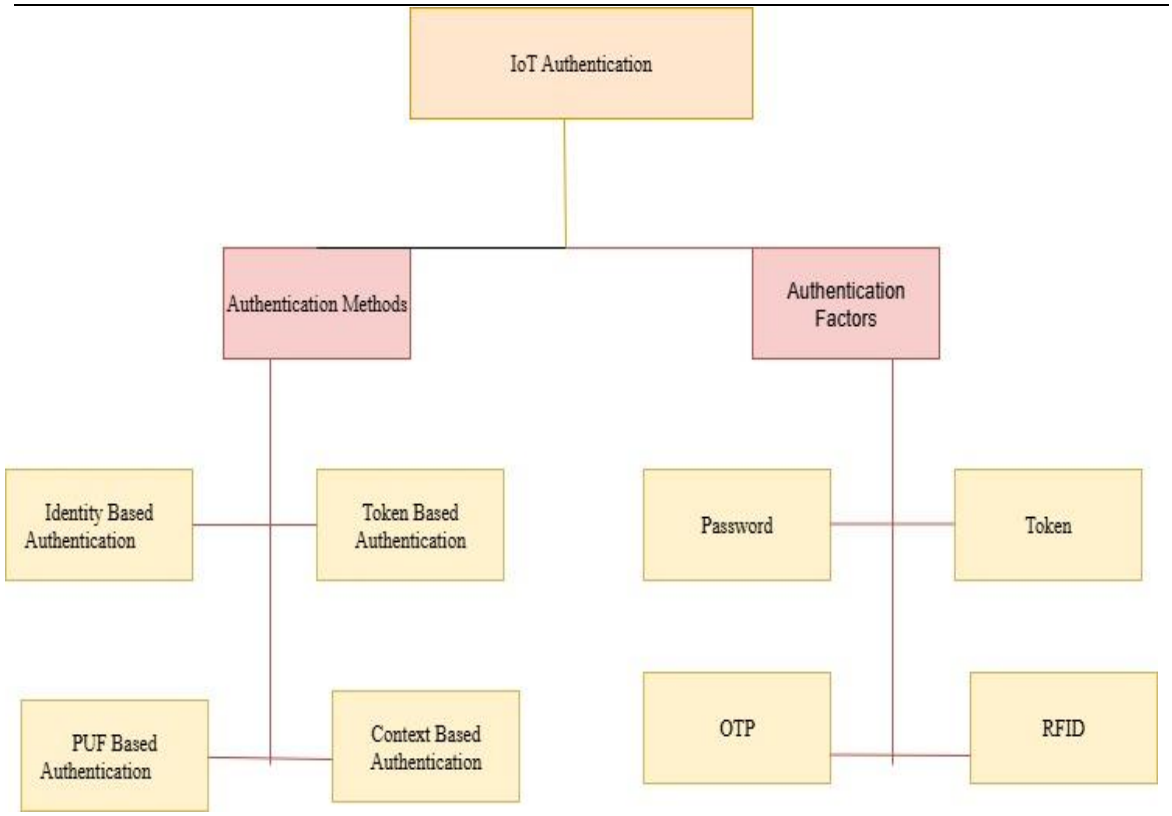

Figure 4: *IoT Authentication Approaches & Factors [16]*

Table 1: *Analysis of Existing Authentication Methods*

Parameter	Identity Based Auth.	Token Based Auth.	PUF Based Auth.	Context Based Auth
Basic Principle	Confirms Identity of a User/ device by using credentials such as User names/ Password.	Uses a time-bound token generated after a successful login to confirm identity of User/ Device	Uses unique hardware-based physical characteristics	Uses environmental or situational data such as user location, time of access, or behavioral patterns to validate identity
Authentication Factor	Knowledge-based (what you know)	Possession-based (what you have)	Hardware-based (what you are—Challenge/Response)	Environment-based (situation-aware)
Resource Requirements	Low	Medium	Medium to High	Medium
Security	Low- chances of password leakage	Medium- For particular session, tokens will be generated	High- No need to store any credentials into the device memory	Low
Strengths	Easy to deploy &Implement	Stateless & Flexible	Strong Hardware based solution, difficult to clone unique characteristics of the device	Enhances security without user involvement
Weakness	Vulnerable to Key stolen Brute force. Spoofing attacks	Vulnerable to Interception, Spoofing, MITM attacks	Vulnerable to Interception, Modeling attacks & also expensive approach	Vulnerable to physical attacks– Context Spoofing attack.

II. Authentication Factor

Authentication factors are divided into four categories, based on the most commonly used methods identified in recent research studies.

1. **One Time Password**: A one-time password (OTP) is a password that changes dynamically for each session, login attempt, or transaction, and is generated based on pre-shared information between two parties. Unlike reusable passwords, OTPs offer strong protection against a variety of security threats [24].
2. **Smart Card**: Smart cards, which have built-in integrated circuits, are commonly used for access control. They are considered one of the most favoured possession-based authentication factors because of their ease of use [24].
3. **Password**: Unique ID/ Value will be used for verification of device legality. Password-based authentication in IoT requires users or devices to provide a username and password to verify their identity. This approach serves as a basic security measure, helping to ensure that only authorized individuals or systems can access and communicate with IoT devices and their associated data [24].
4. **RFID**: RFID is a widely adopted technology, commonly used as a possession-based factor in authentication protocols. It operates using an RFID tag or card along with an RFID reader. Many IoT authentication frameworks incorporate RFID due to its low cost and the fact that it functions without requiring active user involvement [24].

III. State of the Art in IoT Authentication

Several innovative approaches have been proposed in recent years to improve authentication and authorization in IoT systems:

1. **Auth Network Model**: A semi-centralized, globally distributed model named "Auth" was proposed for managing authentication and access control [1]. In this system, each registered device's credentials and corresponding access policies are stored locally in a secure database. The model integrates Public Key Infrastructure (PKI) and digital certificates to validate device identity.
2. **Device Fingerprinting via Communication Patterns**: A novel method was suggested that identifies devices based on communication behaviour and characteristics [2]. The process involves three steps: collecting communication data, extracting relevant features, and calculating attribute similarities to recognize the device type and model.
3. **User Authenticated Key Management Protocol (UAKMP)**: This protocol targets collective IoT networks and uses a combination of smart cards, passwords, and biometric information [3]. It incorporates cryptographic hash functions and private encryption to authenticate users. The UAKMP process involves six stages:
    1. Offline node registration
    2. User enrolment
    3. User login
    4. Authentication and key exchange
    5. Updating password and biometrics
    6. Deployment of newly added sensing nodes
4. **Physical Layer-Based Authentication**: Another method employs physical properties such as Received Signal Strength Indicator (RSSI) and Channel Impulse Response (CIR) for verifying identity [4]. Machine learning techniques are utilized to perform authentication based on these features. Physical Layer Authentication (PLA) offers quick and lightweight

authentication with minimal signalling overhead. However, its authentication accuracy is generally lower compared to cryptographic methods.

5. **Token-Based Security with Energy-Aware Trade-Off**: A dynamic security model was proposed that balances energy usage with required security levels for different types of data and operations [5]. In this approach, clients receive access tokens from the Authorization Server (AS), which specify the scope, duration, and permissions—eliminating the need for static key storage.
6. **Lightweight Two-Factor Authentication**: A privacy-preserving, resource-efficient two-factor authentication scheme was developed to suit constrained IoT environments [6]. It uses a shared secret key along with a PUF to enhance resistance against physical and side-channel attacks.
7. **PUF and Hardware Fingerprints**: A two-factor method integrating PUFs and hardware fingerprints was introduced to strengthen authentication against spoofing and impersonation, especially in low-cost devices [7].
8. **Password and Smart Card-Based Authentication**: To overcome vulnerabilities in password-only methods, a hybrid scheme using both passwords and smart cards was proposed [8]. This combination reduces risks like password guessing attacks.
9. **Biometric and Private Cryptography-Based Scheme**: A multifactor system was presented that generates biometric passwords from user credentials and combines them with private cryptography for user authentication and key exchange [9].
10. **Digital Signature and Device Capability-Based Authentication**: Another proposed method relies on digital signatures and the inherent capabilities of a device to establish secure authentication [10].
11. **Password, Smart Card and Biometrics Based Authentication**: The proposed protocol consists of four main phases: (1) Initialization of the Gateway Node (GWN), (2) Registration of sensor nodes, (3) User registration, and (4) Login and user authentication phase [11]. Proposed protocol offers security against Impersonation attack, Replay attack, MITM attack. However proposed procedure consists of three factors so it requires more computational & communication cost. So, it is inappropriate for resource constrained IoT network.

Table 2: *Analysis of Existing Authentication algorithms from LR*

Sr. No.	Title	Layer	1	2	3	4	5	6	7	8	9
1	Hokeun Kim et al. [1]	A	0	0	0	1	1	1	N/A	0	0
2	Mohammad Wazid et al. [3]	A	0	1	1	0	0	0	N/A	0	0
3	Ning Wang et al. [4]	P	N/A	1	0	0	0	0	N/A	1	0
4	ProsantaGope et al. [6]	A	1	1	0	0	0	0	1	0	0
5	Naveed Aman et al. [7]	A+P	1	1	0	0	0	0	0	1	0
6	Yan Zhao et al. [8]	A	0	1	1	0	0	0	N/A	0	0
7	Majid Alotaibi et al. [9]	A	0	1	1	0	0	1	N/A	0	0
8	NoquiaFateemaTarin et al. [10]	P	1	1	0	0	1	1	N/A	0	0
9	Sachin Taneja et al. [5]	A	1	0	0	1	0	1	0	0	0
10	Liu et al [11]	N+A	0	1	1	1	0	1	0	1	0

Where, P= Perception Layer, N= Network Layer and A=Application Layer
0= Attack not addressed, 1=Attack addressed
Column Heading:
1=Key stolen attack/ Password leakage attack
2= Impersonation attack

3= Replay attack
4= DOS attack
5= Interception attack
6=MITM attack
7= Modeling attack
8= Spoofing attack
9=Physical attack- changing distance attack & same-device type attack

IV. Open Issues in IoT Authentication

Analysing a wide range of authentication protocols and schemes reveals several critical requirements and challenges that must be addressed by researchers and developers when designing new authentication mechanisms for IoT networks and applications. Here are some of them.

1. In sensor-centric applications—where devices are limited in memory, processing capability, and battery life—authentication protocols should be lightweight, carefully balancing security with power consumption.
2. It is essential to ensure that authentication protocols are resilient against various attacks, such as Sybil attacks, node capture, replay attacks, password guessing, message forgery, brute-force attacks, man-in-the-middle (MITM) attacks, Denial of Service (DoS), collision, and chosen-plaintext attacks. Special attention should be given to Distributed Denial of Service (DDoS) attacks, which ranked as the second most frequent attack on IoT systems in 2017 [6].
3. Minimizing communication overhead is crucial, especially for power-constrained devices. This includes reducing the number of message exchanges required during authentication and keeping message sizes small due to limited bandwidth in wireless communication protocols.
4. Low computational overhead is another vital consideration in the design of authentication systems for IoT, emphasizing the need for lightweight cryptographic techniques that suit resource-restricted environments.
5. Scalability is a fundamental requirement—authentication schemes should support a large number of nodes and allow seamless addition of new devices without extensive reconfiguration.
6. The authentication framework should operate effectively across all three layers of the IoT architecture: application, network, and perception.
7. Device heterogeneity across IoT ecosystems must be accommodated, ensuring compatibility and adaptability across different platforms.
8. Hardware-based security mechanisms like Physical Unclonable Functions (PUFs) are gaining popularity due to their enhanced security benefits over software-based approaches. A hybrid model combining software (cost-effective) and hardware (more secure) solutions is recommended for robust IoT authentication.

III. Research Gap & Problem Statement(s)

I. Research Gap

Authentication is critical in IoT networks to ensure only authorized users and devices are granted access, effectively preventing common attacks such as impersonation, replay, and man-in-the-

middle (MITM) threats. After evaluating various existing authentication mechanisms, several shortcomings were identified:

1. **Risk of Credential Theft**: Many current systems remain susceptible to stolen verifier attacks, where credentials or authentication data are intercepted or extracted.
2. **Node Capture and DoS Vulnerabilities**: Several approaches fail to provide defence against physical node capture or denial-of-service (DoS) attacks.
3. **Replay Attack Exposure**: Authentication responses in some methods can be reused by attackers, allowing unauthorized access through replay attacks.
4. **Weakness Against Device Impersonation**: Smart card theft and sensor impersonation remain valid threats in multiple schemes, particularly where device secrets are stored or shared insecurely.
5. **Physical Attacks Based on Location Tampering**: Attacks like location spoofing or distance manipulation can deceive systems by altering the context in which the device is expected to operate.

From the literature, it's evident that most IoT authentication techniques focus on one of the following: cryptography, passwords with smart cards, device behaviour, or hardware features. However, none of the reviewed methods incorporate contextual information—such as device location—as a factor in the authentication process. This is a major oversight.

For example, if a device's location is altered by an attacker (e.g., moved from its operational site in an industrial setting), it could generate false or dangerous outputs. This violates the fundamental principle of authentication and poses a serious safety risk in industrial or health-critical IoT applications.

Therefore, location verification must be integrated into the authentication process to detect physical movement or tampering. Additionally, session-based key generation mechanisms should be adopted to combat key theft. Using dynamic session keys can significantly enhance security against interception and eavesdropping attacks.

Another major gap is that no current solution simultaneously addresses multiple security pillars—confidentiality, integrity, and authentication (CIA)—in a lightweight and power-efficient manner. A new approach combining context-awareness and dynamic key generation could bridge these security gaps and deliver comprehensive protection against a wide range of threats, including interception, replay, and physical attacks.

II. Problem Statements

Securing the identity of IoT devices and the integrity of their data transmissions is central to maintaining a trustworthy IoT ecosystem. As IoT expands into homes, workplaces, industries, and public domains, its open and interconnected nature introduces significant security vulnerabilities. Malicious actors can exploit this openness through attacks such as Denial-of-Service (DoS), replay, side-channel attacks, key theft, and physical tampering.

These attacks compromise the three essential security pillars of any IoT system:

1. **Authentication**: Verifying that a device or user is legitimate.
2. **Confidentiality**: Ensuring that data remains secure during transmission.
3. **Integrity**: Guaranteeing that data is not altered or tampered with.

Without robust security measures, IoT applications lose their effectiveness and cannot be trusted in critical areas like healthcare, industry, etc. Among these pillars, authentication serves as the foundation. If identity verification is weak, unauthorized entities can enter the system, inject malicious data, or interfere with device behaviour. Therefore, a well-designed authentication system is key to defending against attacks such as key theft, MITM, and location spoofing.

Based on the literature review and current trends in IoT security, the following problem statements have been identified:

1. **Problem Statement 1:**Most existing authentication methods rely heavily on static credentials like passwords or pre-shared keys. While easy to implement, these methods are vulnerable to several attacks such as password leaks, replay, eavesdropping, and MITM attacks. Moreover, they do not guarantee unique device identification, making systems prone to physical tampering and location spoofing. Hence, a multi-factor authentication model that includes:Contextual parameters (like device location) and Cryptography-based mechanisms is urgently needed.
2. **Problem Statement 2:**Traditional key-based systems are vulnerable to key theft and brute-force attacks. To counteract this, a multi-key authentication scheme should be developed in which keys are generated dynamically per session. This method must follow a "One-time, One-cipher" principle, ensuring keys are refreshed every session. Current dynamic key generation models—often based on physical properties or LFSR (Linear Feedback Shift Registers)—do not offer strong enough protection and remain predictable.
3. **Problem Statement 3:**IoT devices operate with limited computational power, memory, and energy. This makes it impractical to implement conventional cryptographic algorithms Symmetric & Asymmetric such as DES, AES, or ECC due to their high processing and memory demands. As a result, there is a pressing need to design lightweight encryption and authentication algorithms. These should:
    - Consume minimal power and storage,
    - Communication & Computational cost should be minimum
    - Operate efficiently on constrained hardware, and
    - Still defend against known attacks like key theft, eavesdropping, MITM, and physical intrusion.
4. **Problem Statement 4:**Several researchers have explored the use of password or identity-based authentication methods to enhance IoT network security. In such approaches, a unique value, parameter, or key is employed as the authentication factor. However, a major concern lies in securely transmitting this password or key between the device and the server, and vice versa. This highlights the necessity for a secure key distribution mechanism that ensures safe transmission while minimizing resource consumption—an important consideration in IoT environments with limited computational capacity. Additionally, the issue of key generation/key management must be addressed. Using the same key for an extended period increases the risk of key compromise, especially given IoT's inherently open and exposed architecture.
5. **Problem Statement 5:**The increasing diversity and number of IoT devices present significant challenges in reliably identifying and authenticating each device. Traditional cryptographic techniques often face difficulties with scalability and limited device resources. This study focuses on creating a machine learning-based device fingerprinting approach that can accurately and uniquely recognize devices using their network behaviour or hardware-specific characteristics.

IV. Experimental Results

To evaluate performance and efficiency, commonly used block cipher algorithms—DES, AES, and RC5—were implemented. The focus was to measure key performance metrics relevant to IoT environments, which are typically constrained by power, processing speed, and memory.
The parameters assessed include:

1. Time Required for Encryption: The duration each algorithm takes to encrypt a single data block.
2. CPU Cycles Consumed: The number of processor cycles used during the encryption process.
3. Memory Usage: The storage space required to implement the cipher on a device.

For the experiments, the following block sizes were considered: 1)AES: 128-bit block size and 2) DES and RC5: 64-bit block size.

According to experiments we had following findings: 1) AES performed the best in terms of speed and CPU efficiency, requiring the least amount of time and processor cycles to encrypt data. 2) RC5, despite its simplicity and low memory usage, consumed the most CPU cycles and had the longest execution time. 3) DES, while somewhat faster than RC5, still lagged behind AES in terms of overall efficiency

Table 3: *Existing Cipher Performance Comparison*

Sr. No.	Name of Cipher	Time required for Encryption	CPU Cycles Required	Storage Space Required
1	DES	5.4	55700	160 Bytes
2	AES	2.8	13500	176 Bytes
3	RC5	8.2	92300	104 Bytes

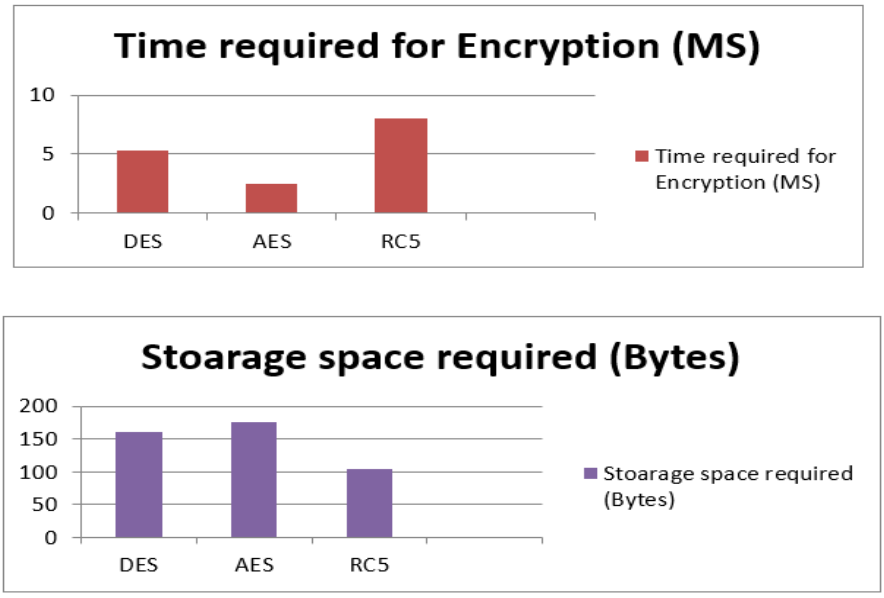

Figure 4: *Comparison for Existing Cryptographic Algorithms Performance*

V. Conclusion

In today's hyper-connected world, billions of IoT devices are integrated into the Internet, opening the door to a wide range of security risks. Ensuring the protection of these devices and the data they generate has become a pressing area of research. This paper provides a comprehensive overview of IoT systems, covering their architecture, components, and the significant security challenges they face. A detailed review of existing literature was conducted to understand various authentication mechanisms currently in use. Through this comparative analysis, we identified critical limitations and vulnerabilities in traditional approaches—especially their inability to resist

advanced attacks like location spoofing, key theft, and monitoring. We have also derived different open issues present currently for the researchers into the domain of IoT Authentication- Multi-factor authentication, integration of context information to enhance the security, lightweight cryptographic solution & adaption of ML to improve the results of authentication service in IoT network. Finally, we have measured the performance of well-known cryptographic algorithms-DES, AES & RC5 in IoT network & concluded with the finding- AES is more suitable in comparison with DES & RC5.

References

[1] Hokeun Kim and Edward A. Lee (2017). Authentication and Authorization for the Internet of Things,IEEE Internet of Things Journal, 19: 27-33.

[2] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, Minho Jo (2017). Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks,IEEE Internet of Things Journal, 5:269-282.

[3] Ning Wang, Ting Jiang, ShichaoLv and Liang Xiao, Senior Member (2017). Physical-Layer Authentication Based on Extreme Learning Machine. IEEE Communications, 21:1557-1560.

[4] Muhammad Naveed Aman, Sachin Taneja, Biplab Sikdar, Kee Chaing Chua, and Massimo Alioto (2019). Token-Based Security for the Internet of Things WithDynamic Energy-Quality Tradeoff,IEEE Internet of Things Journal, 6:2843-2859.

[5] Vikas Hassija, Vinay Chamola ,Vikas Saxena , Divyansh Jain, Pranav Goyal, And Biplab Sikdar (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,IEEE Access, 7:82721-82743.

[6] Prosanta Gope and Biplab Sikdar (2018). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices,IEEE Internet of Things Journal, 6:580-589.

[7] Sulabh Bhattarai and Yong Wang (2018). End-to-End Trust and Security for Internet of Things Applications,IEEE Computer Society, 51:20-27.

[8] Muhammad Naveed Aman, Mohamed Haroon Basheer and Biplab Sikdar (2019). Two factor Authentication for IOT with Location Information,IEEE Internet of Things Journal, 6(2): 3335-3351.

[9] Yan Zhao, Shimming Li and Liehui Jiang (2018) Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multi-server Environment,WILEY Hindawai Security and Communication Networks, 18:1-13.

[10] Majid Alotaibi (2018). An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN,IEEE Access, 6:70072-70087.

[11] Zahoor Ahmed Alizai, Noquia Fatima Tareen and Iqura Jadoon (2018). Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures,IEEE International Conference on Applied and Engineering Mathematics.

[12] Moritz Loske, Lukas Rothe and Dominik Gertler (2019). Context-Aware Authentication: State-of-the-Art Evaluation and Adaption to the IIoT,IEEE 5th World Forum on Internet of Things (WF-IoT), https://doi.org/10.1109/WF-IoT.2019.8767327.

[13] Armin Babaei, Gregor Schiele (2019). Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges,Sensors, 19 (14):3208 https://doi.org/10.3390/s19143208.

[14] Baibhab Chatterjee, Shovan Maity (2019) RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-situ Machine Learning, IEEE Internet of Things Journal, 6(1): 388-398.

[15] Tarak Nandy, Norjihan Abdul Ghani and Sananda Bhattacharya (2019). Review on Security of Internet of Things Authentication Mechanism,IEEE Access, 7: 151054-151089.

[16] Santosh Krishna B V and Gnanasekaran T (2017). A Systematic Study of Security Issues in Internet-of-Things (IoT), IEEE International conference on I-SMAC, https://doi.org/10.1109/I-SMAC.2017.8058318.

[17] Mardiana binti Mohamad Noor, Wan Haslina Hassan (2019). Current research on Internet of Things (IoT) security: A survey, ELSEVEIR Computer Networks, 148: 283-294.

[18] Chang-le Zhong, Zhen Zhu and Ren-gen Huang (2017). Study on the IOT Architecture and Access Technology,IEEE 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, https://doi.org/10.1109/DCABES.2017.32.

[19] Jeffrey Voas, Bill Agresti (2018). A Closer Look at the IoT's "Things", IEEE Computer Society, 20 (3): 11-14.

[20] Jyoti Deogirikar and Amarsinh Vidhate (2017). Security Attacks in IoT: A Survey,IEEE International conference on I-SMAC, https://doi.org/10.1109/I-SMAC.2017.8058363.

[21] Zhiping Jiang, Kun Zhao and Junzhao Du (2020). PHYAlert: identity spoofing attack detection and prevention for a wireless edge network, Journal of Cloud Computing, 9 (5):1-13.

[22] I. Cetintav and M. Tahir Sandikkaya (2025). A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs, IEEE Access, 13: 37703-37723, doi: 10.1109/ACCESS.2025.3546147

[23] N. Sharmila Kumari, H. S. Vimala, C. N. Pruthvi and J. Shreyas (2024). Holistic Survey on Security in IoT Application Layer: Attacks, Protocols, and Applications, IEEE Access, 12: 186957-187014, doi: 10.1109/ACCESS.2024.3462170

[24] M. S. Rajan, J. R. Arunkumar, A. Ramasamy and B. Sisay (2021). A comprehensive study of the Design and Security of the IoT layer Attacks, 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India,doi:10.1109/ICCES51350.2021.9489235.

[25] R. R. Pahlevi, V. Suryani, H. H. Nuha and R. Yasirandi (2022). Secure Two-Factor Authentication for IoT Device, 10th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, doi: 10.1109/ICoICT55009.2022.9914866.

[26] N. T and L. R (2024), Designing a Lightweight IoT Authentication Protocol for Resource-Constrained Devices, International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, doi: 10.1109/ICICAT62666.2024.10923434.

[27] V. K. Rai, S. Tripathy and J. Mathew (2023). LPA: A Lightweight PUF-based Authentication Protocol for IoT System, IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications Exeter, United Kingdom, doi: 10.1109/TrustCom60117.2023.00233.

[28] A. N. Alsheavi(2025). IoT Authentication Protocols: Classification, Trend and Opportunities, IEEE Transactions on Sustainable Computing, 10(3): 515-533, doi: 10.1109/TSUSC.2024.3492152.

[29] I. Cetintav and M. Tahir Sandikkaya (2025). A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs, IEEE Access, 13:37703-37723, doi: 10.1109/ACCESS.2025.3546147.