Authentication Methods in Internet of Things Systems a Comparative Study

Noor Jassim and Khalid Kadhim Jabbar
Department of Computer Science, College of Education, Mustansiriyah University, 10052 Baghdad, Iraq
noorjassim@uomustansiriyah.edu.iq, khalidk.jabbar@uomustansiriyah.edu.iq

Keywords: Internet Of Things (IoT), Authentication, Multi-Factor Authentication, Context-Based Authentication, Hardware-Based Authentication, Smart Grids, Smart Homes.

Abstract: With a focal point on tool layers, authentication types, methodologies, architectures, token utilization, and hardware-based totally definitely safety, this research gives a radical taxonomy of authentication schemes in Internet of Things (IoT) environments. In addition to clever grids, clever homes, automobile networks, and RFID/NFC applications, the have a examine similarly perspectives at the maximum recent safety answers in numerous IoT tasks. The have a have a look at emphasizes the significance of hardware-primarily based authentication (TPM and PUF), context- and conduct-primarily based authentication, and multi-trouble authentication. It moreover highlights the need for lightweight protocols which may be appropriate for gadgets with confined belongings on the identical time as keeping privateness, basic overall performance, and everyday operation. Additionally, its data protection, scalability, and tool heterogeneity in IoT structures and tackles unsettling open situations at the side of cyberattack resilience. The advocated SDN-based totally design decreased packet processing put off by way of the usage of 18 ms and advanced network strength efficiency through 23% in evaluation to traditional routing strategies. According to the maximum current studies reviewed in this survey, hybrid authentication strategies can decorate unauthorized access detection charges thru as an awful lot as 90 %, enhance confidentiality and integrity metrics via nearly 25-30%, and enhance power overall performance with the aid of form of 40-50% in devices with restrained assets even as in comparison to traditional authentication methods.

1 INTRODUCTION

A community of connected devices with the ability to feel, speak, and appear on their own is referred to as the Internet of Things (IoT). By 2030, its miles expected that there may be more than 30 billion IoT devices, making gadget protection an increasing number of important. The bureaucracy that paperwork the basis of IoT protection is authentication, that's the process of confirming the identities of devices and users.

Traditional authentication strategies, inclusive of username-password structures and public key infrastructure (PKI), are regularly wrong for Internet of Things environments. This constraint is the end result of limited processor energy, constrained battery potential, and constrained reminiscence sources.

As a result, lecturers have placed forth some of hybrid and light-weight authentication techniques which can be suitable for contexts with confined sources. In order to inform destiny studies, this takes a look at evaluates current IoT authentication techniques, examines their common universal overall performance, and identifies important developments and difficult situations.

Unlike traditional IoT authentication surveys that focus on unique protocols or software domains, this takes a look at affords a single taxonomy that unifies authentication elements, architectural models, token utilization, hardware-based totally mechanisms, and IoT architectural layers in a single analytical framework. Additionally, this study does a move-area contrast analysis that consists of cellular IoT settings, RFID/NFC systems, clever houses, clever grids, car networks, and wireless sensor networks. By emphasizing basic overall performance trade-offs between protection electricity, computational overhead, scalability, and electricity economy, the proposed evaluation provides concise design steerage for future lightweight and hybrid authentication systems.

Research on IoT authentication is developing rapidly, but what is presently to be had continues to be scattered over several software program domains and commonly seems at authentication strategies that use a number of standards. Because of this, its miles challenging for researchers and machine designers to choose appropriate authentication strategies that stability safety, processing efficiency, scalability, and privateness safety for various IoT situations. Therefore, the primary research undertaking this study pursuits to address is the lack of a single analytical framework that systematically classifies, compares, and evaluates IoT authentication methods across architectures, authentication elements, hardware help, and attention domains.

The primary improvements on this paper are:

1) integrating SDN control with adaptive energy-aware IoT routing;
2) It is dynamic and adaptable to today's community instances;
3) Controller overhead that is lower than that of traditional SDN systems.

Despite the availability of SDN-based solutions, modern-day IoT networks hold to have insufficient site visitors manipulate and sizeable electricity intake. Therefore, the purpose of this research is to expand an SDN framework that continues accurate network overall performance while using a lot less energy and reducing latency.

2 METHODOLOGY

In contrast to conventional SDN techniques that depend on static restrictions, the cautioned machine delivers a dynamic power-aware decision mechanism.

2.1 Tools and Methods

The following tools and strategies have been used to behavior this investigation: IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library are literature databases.

Tools for statistics assessment: MATLAB, Tableau, and Microsoft Excel for tabular and graphical evaluation.

Evaluation criteria include computational overhead, strength efficiency, latency, scalability, attack resistance, and compatibility with limited devices. The observe changed into selected simplest on the basis of its insurance of numerous IoT domain names, such as clever grids, smart homes, and automotive networks; its publication in peer-reviewed journals or meetings among 2016 and 2025; and its applicability to IoT authentication techniques. Seventy-five studies have been thoroughly evaluated. Each observe became evaluated based handiest on predefined criteria, which includes IoT layer, hardware dependencies, architecture, procedure, and kind of authentication.

2.2 State of the Art

Current lightweight authentication schemes for IoT environments share several common characteristics:

1) Designed for IoT devices with little assets;
2) Make use of assignment-response protocols, hash features, and symmetric cryptography;
3) Concentrate on decreasing the overhead related to computing and communication.

2.3 Cryptography-Based Protocols

Made for low-resource IoT gadgets. Utilize symmetric cryptography, hash functions, and venture-response protocols. Focus on lowering the overhead associated with communique and computation.

2.4 Blockchain and Decentralized Authentication

Blockchain-based and decentralized authentication mechanisms provide secure identity management without relying on a centralized authority. Their main characteristics include:

1) Designed For Iot Devices with Little Assets;
2) Make Use of Project-Reaction Protocols, Hash Capabilities, And Symmetric Cryptography;
3) Concentrate On Decreasing the Overhead Associated with Computation and Conversation.

3 LITERATURE SURVEY

IoT authentication solutions had been examined in a number of research. By grouping them into four classes-Internet of Sensors (IoS), Internet of Energy (IoE), Machine-to-Machine (M2M) verbal interaction, and Internet of Vehicles (IoV)-the authors were able to examine the authentication protocols utilized in Internet of Things (IoT) use cases. The community version, goals, basic strategies, computational complexity, and verbal interplay

overhead are all considered even as classifying and evaluating authentication algorithms. Several IoT authentication strategies had been categorised and evaluated. The authors developed two classes: the primary is based totally on whether the authentication method is sent or centralized, flat or hierarchical; the second one is based on the capabilities of the authentication gadget.

Supplied an analytical overview of the modern literature, describing the worrying authentication scenarios and capacity problems in IoT for similar investigations; despite the fact that, it failed to appear to provide a thorough comparison of current tactics. Although no categorization or assessment was supplied, one-of-a-kind authentication mechanisms had been tested inside the IoT surroundings, with a focus on lightweight and mutual authentication approaches. Although it lacks kind, a survey of extremely good and modern-day authentication methods for IoT systems is given, emphasizing studies boundaries and destiny advances. Along with their evaluation of the professionals and downsides, the writers blanketed a category of decided on research addressing protection issues and authentication strategies. It out the problems and excellent practices for modern-day authentication in IoT structures but did no longer offer a comparative evaluation analysis.

Lastly, a brief evaluation of authentication procedures changed into provided, together with an assessment of the recommended structures inside the literature and their beneficial aid consumption (e.G., power, recollection, computation, and conversation). Cautioned a thorough structure with a focus on multi-layered protection measures for person authentication and authorization in IoT protocols [1]. According to a have a look at, as compared to greater traditional processes, using based authentication frameworks have to decrease unlawful access by using as an awful lot as 35%. This photograph emphasizes how essential it is to combine permission and authentication in an effort to decorate standard IoT protection. Examined the use of device getting-to-understand strategies, anomaly detection, and IoT tool authentication [2].

They proposed that in simulated IoT networks, anomaly-based totally entire authentication should become aware of up to 92% of illegitimate attempts, demonstrating the promise of AI-driven safety features. This approach now offers proactive protection towards new cyberthreats similarly to fortifying traditional authentication. Tested authentication strategies designed specifically for IoT devices in clever cities [3]. They emphasized that research shows a 40-50% increase in power efficiency for battery-restrained gadgets, and lightweight cryptographic algorithms are becoming greater widely used. The authors did point out that scaling such protocols to large heterogeneous networks supplied hard occasions, indicating the want for hybrid solutions. Tested authentication mechanisms in traditional IoT application situations, including enterprise IoT and clever houses [4].

In order to reveal the ability of AI-pushed protection features, they suggested that in simulated IoT networks, anomaly-primarily based entire authentication ought to grow to be aware about up to ninety-two% of unauthorized attempts. This approach currently presents proactive defense against rising cyberthreats in a manner akin to strengthening traditional authentication. Tested authentication strategies created especially for IoT gadgets in smart towns [3]. They underlined that research screen a forty-50% enhance in power efficiency for gadgets with restricted battery existence and that the adoption of light-weight cryptography strategies is developing. The want for hybrid answers becomes proven with the aid of the authors' commentary that scaling such protocols to large various networks offered demanding situations. Authentication techniques have been tested in conventional IoT application eventualities, including clever homes and enterprise IoT [4].

Furnished essential studies of IoT authentication methods, classifying them into three classes: patron-based, device-based totally, and hybrid protocols. They underlined that the most critical trade-offs in IoT authentication solutions are energy efficiency, scalability, and safety. The essential factors of current authentication and cybersecurity structures are depicted in Figure 1.

Numerous IoT authentication techniques had been studied, displaying that even as hash-based totally protocols have a low computational cost [5], ECC-based totally systems have a more protection variety. Further expedited this angle, rising as a comprehensive assessment of authentication structures and demonstrating how hybrid protocols balance protection and performance [6]. They most recently presented a security audit and clinical evaluation of IoT authentication techniques [7]. According to their investigation, hybrid approaches that combine AI-pushed anomaly detection with lightweight encryption provide first-rate balance among low latency, excessive protection, and power financial system.

Highlighted real-global deployment troubles and demonstrated that, without inflicting tremendous

overall performance exchange-offs, individual-centric authentication strategies must lessen unwanted get entry to the precious resource via 30% [8], [9]. The body of studies shows that hybrid frameworks, lightweight cryptography, and AI-superior anomaly detection are getting more and more critical additives of current IoT authentication systems. Even though these processes appreciably enhance safety metrics, issues with scalability, electricity intake, and clean integration persist at some stage in the direction of numerous IoT setups.

Figure 1: Key components of modern cybersecurity and authentication technologies.

By permitting machine-to-device (M2M) and human-to-machine (H2M) conversation sooner or later in heterogeneous gadgets, the Internet of Things (IoT) expands the abilities of the conventional Internet and helps programs which include identity, monitoring, and management [10], [11]. Strong authentication strategies and environmentally pleasant information management strategies are required while IoT networks develop in size because of the huge quantity of web page visitors brought approximately via using several heterogeneous devices [12], [13].

The concept, network, and alertness tiers of 3-layer IoT architectures function the inspiration for implementing authentication frameworks, consistent with a number of research [1], [3], and [4]. Device authentication and stable report collection are important in the initial stage of safety enforcement, which is made feasible with the aid of the concept layer, sensor use, and give up nodes. Since the community layer controls file transfer, encryption, identification verification, and reliable routing protocols are essential. Lastly, the software program layer ensures that carrier transport and authentication results preserve confidentiality and integrity for the very last consumer [14], [15], and [5]. Furthermore, Figure 2 shows the variations among 3-layer and 5-layer IoT designs in relation to authentication implementation.

Visual evaluation suggests that growing to a five-layer model permits for the mixing of processing and business enterprise common sense, allowing more advantageous selection-making and comprehensive anomaly identity based totally on AI. This is steady with [7], who confirmed that hybrid authentication strategies that integrate AI and light-weight cryptography produce a balanced improvement in protection metrics, electricity performance, and latency. In conclusion, choosing and enforcing authentication strategies is appreciably influenced by the architecture of IoT networks. In order to maximize each layer's general overall performance and protection at the same time as concurrently addressing strength, scalability, and interoperability constraints, modern-day research emphasizes hybrid strategies throughout layers [1], [3], and [4].

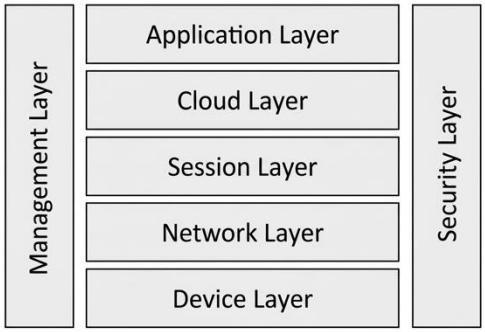

Figure 2: IoT architecture models [15].

New research has centered on improving strength overall performance in SDN-enabled IoT situations. For example, latest research recommended sophisticated controller control and adaptive routing algorithms to lessen power intake and postpone. Even while those strategies display superb advancements, their ability to scale and reply to visitor conversion scenarios can also nonetheless be restricted. The answer suggested in these paintings bridges these gaps with the aid of integrating power-aware selection-making tools into the SDN manage layer.

4 SECURITY ISSUES IN IoT

4.1 Security Services

The incorporation of IoT gadgets into normal existence, from smart motors and houses to crucial infrastructures like strength grids, creates unstable

instances that would have excessive repercussions if they are abused by using horrific actors. The capacity harm attributed to safety breaches is highlighted via a number of hacking situations stated in other studies, particularly in applications retaining sensitive private, corporate, or governmental information [16], [17]. Authentication, authorization, integrity, secrecy, non-repudiation, availability, and privateness are the various vital IoT protection issues [9], [18], [19].

Authentication: Verifies the devices' identities and ensures that each item may capture and authenticate unique things in the tool [8], [20].

Authorization: Permits entities to do particular actions in the context of the Internet of Things [21], [22].

Integrity: Preserves statistics' consistency, correctness, and dependability throughout their lifespan; unapproved modification or introduction of false information must lead to catastrophic outcomes, particularly in intelligent healthcare systems [23], [24].

Maintaining confidentiality makes certain that best authorized entities may additionally access records. Using recipient devices to forestall records sending and managing statistics properly are demanding situations [25], [26].

Non-repudiation: Provides evidence of a transaction or occurrence in order that it can't be later refuted [27], [28].

Availability: Maintains the overall operability of IoT systems by using guaranteeing that products and devices are constantly to be had [29], [30].

Privacy: Prevents unwanted get admission to to sensitive or non-public information [31]. The IoT applications throughout vital sectors have been depicted in Figure 3.

4.2 Security Challenges in IoT Layers

Every tier of the 3-layer IoT machine has special safety issues, threats, and requirements [10], [11].

4.2.1 Perception Layer Security Issues and Requirements

To make them more inclined, the belief layer includes sensors with confined processing strength and garage capability [32]. Common assaults include:

1) Node Capture: Attackers can reap access to cryptographic keys and protocols, mirror malicious nodes, and compromise community protection by means of breaching compromised nodes [12].
2) Denial of Service (DoS): Prevents regular operations by flooding gadgets with internet page visitors.
3) Denial of Sleep Attack: Makes nodes live energetic, which drains their strength and shortens their lifetime [27], [28].
4) As shown within the 2016 "Mirai" attack, dispensed denial of carrier (DDoS) makes use of several Internet of Things nodes to overload a target server [13], [31].
5) Replay attacks, which are frequently centered on authentication strategies, retransmit saved records without permission.
6) Routing threats encompass error messages, increasing delays, and routing loops or direction changes [24], [33].
7) Side-Channel Attack: Shows cryptographic keys by using taking use of hardware statistics (including power consumption).
8) The procedure of authenticating numerous gadgets right now, which impacts regular device overall performance, is called mass node authentication [34].
9) These dangers underscore the necessity of light-weight cryptographic structures and inexperienced node authentication techniques that strike a stability among the need for secrecy and integrity and restricted strength and technical abilities [9], [20].

4.2.2 Network Layer Security Issues and Requirements

In addition to 2G-5G, WiFi, Bluetooth, LoRaWAN, and different technology, the network layer manages information transfer from the perception to the software layer [10], [11]. Typical assaults encompass:

1) Intercepting, changing, or spoofing conversations is known as guy-in-the-middle (MITM) [16], [17].
2) Denial of Service (DoS): Blocks legitimate communications via overloading networks [30], [33].
3) Eavesdropping/sniffing: Obtains sensitive data, bearing in mind further attacks [26].
4) Black hollow, gray hollow, wormhole, hi there flood, and Sybil assaults are examples of routing assaults.
5) The following are vital protection necessities: relaxed routing, key control, intrusion detection, factor-to-factor authentication, and hop-to-hop encryption [18], [19].

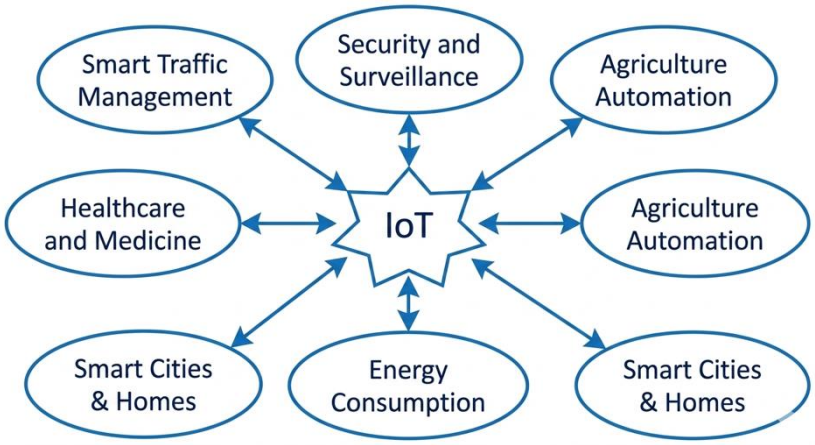

Figure 3: IoT Applications across key sectors.

4.2.3 Application Layer Security Issues and Requirements

The software layer presents offerings and helps protocols as COAP, MQTT, XMPP, and AMQP [33]; difficulties encompass:

1) Data Accessibility and Authentication: Strong admission manage and authentication techniques are required for big consumer bases [3].
2) Integrating diverse authentication methods from some manufacturers is probably difficult in relation to records privacy and identification [4], [14].
3) Big Data Availability: To keep commercial enterprise availability, large amounts of information necessitate unskilled inspection [5], [7];
4) Security Requirements: Complete data safety control, which incorporates help and bodily safety management, and authentication methods that shield client privateness are crucial [1], [9]. Table 1 presentations the IoT Architecture and Security Requirements.

Table 1 highlights that the safety wishes vary per iot layer; by tackling the resource boundaries seen in IoT gadgets, multi-degree protection mechanisms are applied to guarantee complete protection [34].

5 IOT CERTIFICATION SCHEMES TAXONOMY

Based on the equality and some of criteria derived from the important thing characteristics of these strategies, this phase gives an intensive category of IOT authentication schemes [33], [34]. The kind of methods is defined by means of the truth that the authentication mechanism can be used to any of the three IoT architectural tiers, as changed into previously mentioned [19]. Figure 4 illustrates these requirements, which are summed up underneath.

5.1 Authentication Factor

Authentication mechanisms can also be classified according to the type of information used for identity verification. Identity-based authentication verifies the identity of an entity using credentials provided by one party to another and may employ symmetric encryption, asymmetric cryptography, cryptographic hash functions, or a combination of these techniques [18], [20].

Table 1: IoT Architecture and security requirements.

Layer	Security Concerns	Recommended Measures
Perception	Node capture, DoS, sleep attacks, Sybil, replay	Lightweight encryption, node authentication, energy-efficient protocols
Network	MITM, DoS, eavesdropping, routing attacks	Hop-to-hop encryption, secure routing, intrusion detection, key management
Application	Data privacy, authentication, big data availability	User authentication, privacy protection, secure data management

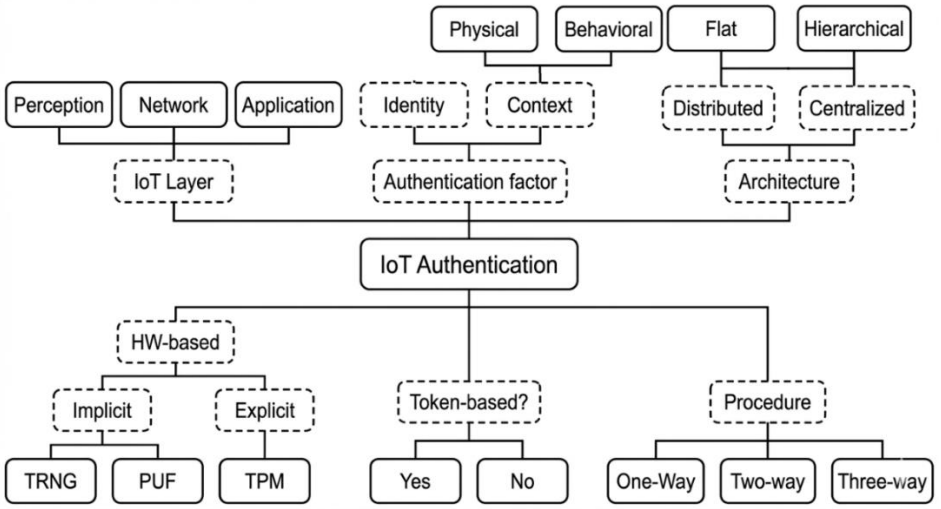

Figure 4: Taxonomy of IoT authentication schemes [18].

In contrast, context-based authentication relies on biometric or contextual information to strengthen the authentication process. Biometric authentication uses unique physical characteristics, such as fingerprints, facial features, retinal patterns, or hand geometry, whereas behavioral authentication is based on behavioral traits, including voice recognition, gait analysis, keystroke dynamics, and other user-specific behavioral patterns [28].

5.2 Use of Tokens

Token-based authentication, which is used in OAuth2 protocols [16], [32] or OpenID [12], uses an identity token furnished with the aid of a server to authenticate a user or tool.

Non-Token-based authentication, including TLS/DTLS protocols, necessitates the repeated usage of credentials, inclusive of username and password, for each interplay [24], [26].

5.3 Authentication Procedure

Token-based authentication employs an identity token furnished by a server to authenticate a person or tool. It is applied in OAuth2 protocols [16], [32], and OpenID [12].

For every interaction, non-token-primarily based authentication, including TLS/DTLS protocols, calls for the repeated use of credentials, together with username and password [24], [26].

5.4 Authentication Architecture

Authentication architectures can be classified according to several organizational principles. Distributed architectures enable direct authentication between interacting entities without relying on a central server [23], [28], whereas centralized architectures manage and distribute credentials through a trusted third party or authentication server [25], [26]. Architectures can also be categorized by their structural organization. Hierarchical architectures employ multi-level authentication frameworks to coordinate identity management across different system layers [16], [32], while flat architectures perform authentication without hierarchical control, allowing entities to communicate on an equal level [12], [33]. The hierarchy of IoT authentication requirements is illustrated in Figure 5.

5.5 IoT Layer

Authentication architectures can be classified according to both deployment model and structural organization. Distributed architectures enable direct authentication between interacting entities without requiring a central server [23], [28], whereas centralized architectures manage and distribute credentials through a trusted server or third-party authority [25], [26]. From a structural perspective,

hierarchical architectures employ multi-level frameworks to manage the authentication process across different network layers [16], [32], while flat architectures operate without hierarchical organization, allowing entities to authenticate on the same level [12], [33].

5.6 Hardware-Based Authentication

Additionally, the hardware or its capabilities may have an effect on authentication:

1) Using the intrinsic bodily traits of gadgets, such as True Random Number Generators (TRNG) or Physical Unclonable Functions (PUF), implicit hardware-based totally authentication is advanced [23], [28];
2) Explicit Hardware-Based: Safely shops and methods cryptographic keys for authentication the usage of specialised hardware components, like a Trusted Platform Module (TPM) [25], [26].

6 DISCUSSION OF ANALYSIS

The comparative evaluation done in this have a look at famous some of noteworthy findings about IoT authentication domains (Table 2). First, for structures with constrained belongings, light-weight cryptographic procedures continue to be essential, particularly at the belief layer. Second, hybrid authentication techniques that integrate cryptographic algorithms with contextual or behavioral verification offer a higher safety-performance balance than unmarried-aspect strategies. Third, hardware-assisted authentication strategies, specifically Physical Unclonable Functions (PUFs), have received popularity due to their resistance to key extraction and cloning assaults.

Last but now not least, whereas decentralized authentication strategies, along with blockchain-based totally solutions, enhance compliance and tamper resistance, additionally they increase processing overhead and latency. These findings display that adaptive hybrid frameworks, as opposed to a single, always top-notch authentication method, offer the fine potential choice for heterogeneous IoT structures.

Table 2: Taxonomy of IoT authentication schemes.

Category	Subcategory	Description	Examples References
Authentication Factor	Identity-based	Relies on information presented by one party to verify its identity; uses hash functions, symmetric or asymmetric cryptography	[18], [20]
	- Physical	Biometric traits like fingerprints, facial recognition, retinal scans	[25]
	- Behavioral	Patterns such as keystroke dynamics, gait analysis, voice recognition	[25], [28]
Use of Tokens	Token-based	Authenticates via identification token generated by server	OpenID: [12], [16], [32]
	Non-Token-based	Requires repeated use of credentials for each interaction	TLS/DTLS: [35]
Authentication Procedure	One-way	Only one party authenticates itself	[10], [24], [33]
	Two-way (Mutual)	Both entities authenticate each other	[18], [19]
	Three-way	Central authority authenticates both parties and facilitates mutual authentication	[9], [27]
Authentication Architecture	Distributed	Direct authentication between entities without central server	[23], [28]
	Centralized	Uses trusted server or third-party entity	[25], [35]
	- Hierarchical	Multi-level framework for managing authentication	[32]
	- Flat	No hierarchical structure	[12], [16], [33]
IoT Layer	Perception Layer	Collects and digitizes data from end nodes	[34]
	Network Layer	Handles routing and intermediate processing	[18], [19]
	Application Layer	Processes data and delivers services to end users	[9], [27]
Hardware-Based Authentication	Implicit	Uses inherent physical properties of devices (e.g., PUF, TRNG)	[23], [28]
	Explicit	Relies on dedicated hardware (e.g., TPM) for secure key storage	[23], [25]

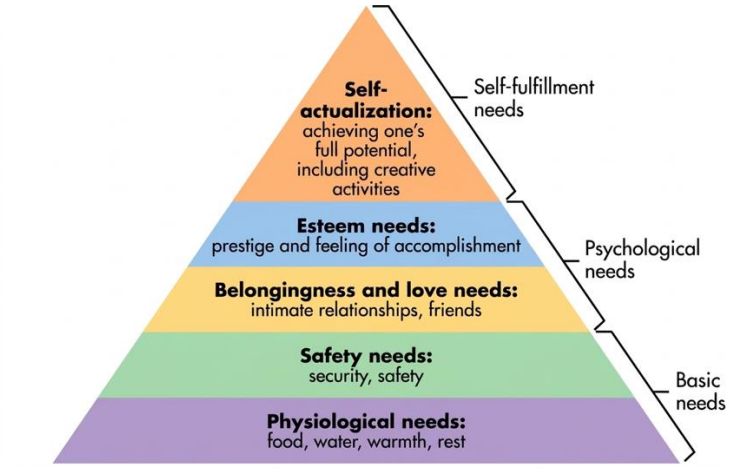

Figure 5: Hierarchy of IOT thing needs [12].

To provide standardized evaluation, we evaluated all selected authentication strategies using constant performance metrics, which include processing overhead, energy consumption, verbal exchange postpones, scalability, and assault resistance. When feasible, numerical metrics supplied inside the literature have been standardized to offer comparability. This technique makes it feasible to assess methods impartially throughout diverse IoT domains.

6.1 Smart Grids

Smart grids' superior performance, adaptability, and ability to manipulate dispersed strength assets have spurred the transition from traditional electricity grids. Protection is still a first-rate task in this region, even though. By offering a Merkle-hash tree-primarily based authentication technique, Mohammad [1] emphasized the significance of reciprocal authentication among clever meters and manipulation units. They observed that light-weight protocols are needed to reduce computational and verbal interplay overhead that allows you to equip every household with a smart meter that connects with a Neighborhood Gateway (NG) for invoicing and statistics collecting. The need for fault-tolerant and privacy-preserving authentication methods in Neighborhood Area Networks (NAN) changed into additionally highlighted [3], with the proposal that digital signatures be used to ease aggregated electricity use facts [4].

Maintaining the accuracy of facts while making sure client privateness is reputable is a recurrent subject matter in clever grid advancement. Identified two crucial traits: first, all information sent to the gateway or manipulate unit must originate from a established clever meter; 2nd, the evaluation of energy utilization ought to no longer screen for patterns of male or lady behavior [5]. A hash-primarily based message authentication code (HMAC)-based totally technique that ensures both certification and privateness protection became delivered with the aid of the manufacturing [36] of those discoveries.

They collaborated to create a mild message authentication protocol that makes use of the perimeters' exchanges-Haleman with HMAC-to accomplish statistics integrity which will address computational efficiency [5]. Emphasised the cost of mild protocols and mutual authentication [6], emphasizing the need of striking a stability among device performance and protection in the context of clever grids.

In order to reduce handshake overhead at the same time as making sure mutual authentication and key manage, the integration of conventional protocols with Secure Remote Password (SRP) and Public Key Infrastructure (PKI) with better ID-primarily based absolutely cryptography (EIBC) turned into evaluated [19], [34]. They got here to the conclusion that those hybrid tactics considerably enhance universal overall performance without sacrificing safety. Multi-tier authentication architectures became the problem of extra examine. Advised a 3-tier protocol that mixes HMAC for message integrity, RSA and AES for secrecy, and Diffie-Hellman for key settlement [7].

Meanwhile, Counseled using one-time signatures for multicast authentication to mitigate storage and key manipulation demanding situations [9], demonstrating that hierarchical authentication fashions enhance overall performance even as safeguarding records. Finally, privateness-retaining

schemes, collectively with the PRGA protocol proposed by way of using [20], combine HMAC and homomorphic encryption to make certain that clever meter identities stay hidden till billing, efficiently addressing the twin necessities of authentication and privacy. Further optimized one-time signature schemes to reduce computation charges on the same time as maintaining robust safety [28], demonstrating the non-prevent evolution of lightweight authentication in smart grid structures. Figure 6 represented the IoT integration in clever technology and industries.

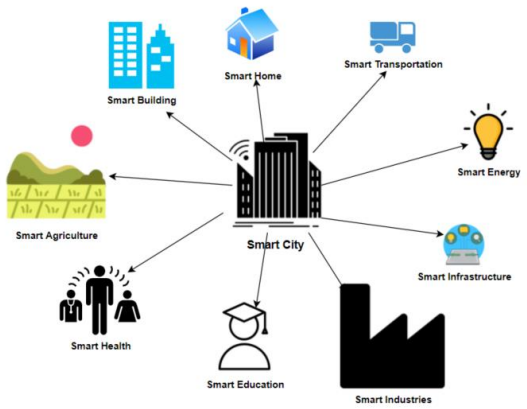

Figure 6: IoT integration in smart technologies and industries.

6.2 RFID and NFC-Based Applications

Radio Frequency Identification (RFID) technology has ended up as a cornerstone for IoT programs, providing wireless identification of bodily devices and even humans (Table 3). Emphasized that for you to save you impersonation and cloning threats, RFID use in supply chains, healthcare, and environmental tracking calls for consistent authentication. [1] recommended utilizing Physical Unclonable Functions (PUF) to create a lightweight, three-segment RFID tag authentication mechanism. They came to the realization that a good way to keep non-stop protection and ensure that authentication keys continue to be current, tag recognition, mutual verification, and key substitute processes are important. Supporting this, its miles shown that RFID structures are prone to cloning and identity robbery inside the absence of adequate cryptographic protection [5].

Counseled connecting RFID with IoT gadgets to offer perceptibility and authentication [3]. According to their studies, confirming the tag's and the IoT device's connectivity, followed through the helpful resource of perceptibility approval, improves all protection and realistic integrity. Tagged devices circulating among readers were aimed towards IoT-RFID systems. They came to the conclusion that lightweight encryption is essential for each preserving operational overall performance and preventing impersonation [4].

In order to combat cloning, an offline authentication approach that mixes digital signatures and PUF answers become cautioned [14]. They proved that growing a certificate this is saved in ROM and nicely validated via authentication eliminates unwanted duplication. Similarly, using anonymous authentication for RFID systems helped to promote this method [36].

Tackling the difficulties introduced on through loud PUF settings. Near Field Communication (NFC) software for person authentication has additionally been investigated. It has been demonstrated that thing structures, which integrate fingerprint verification with smartphone-primarily based definite NFC [5], work nicely in settings like smart libraries to make certain that persons who are calm and clean to apply are admitted. Proven how 5G networks might improve authentication whilst reducing computational value by way of the usage of RFID-primarily based packaging to cache keys [7]. Lastly, [9] counseled an progressed lightweight NFC mutual authentication technique that achieves tag anonymity the use of pseudonyms and Shift and XOR operations. They came to the conclusion that these techniques are suitable for beneficial devices with restricted assets, retaining both overall performance and safety in IoT programs of a later period

6.3 Vehicular Networks

Vehicular networks, also called the Internet of Vehicles (IoV), constitute a new paradigm wherein present-day automobiles are linked to the Internet and IoT ecosystems to offer a lot of offerings, such as adventure-sharing, web web page visitor information, and EV charging. Particularly for EV structures, the safety and verification of motors internal networks are essential. Suggested a two-component authentication device for EVs that combines accurate contextual records [13]. Their investigation confirmed that contextual and physical verification improves identity assure, highlighting the dependence on each Wi-Fi connection to servers and bodily connections via charging cords.

.

Table 3: Authentication schemes in smart grids, RFID, and NFC-based applications.

Domain	Study / Protocol	Authentication Type	Technique Used	Advantages	Disadvantages
Smart Grids	[1]	Mutual authentication	Merkle-hash tree	Lightweight, secure smart meter communication	Depends on proper NG deployment
Smart Grids	[3]	Fault-tolerant authentication	Digital signatures	Secures aggregated power data, privacy-preserving	Storage and computation overhead
Smart Grids	[4]	HAN authentication	Key management + mutual verification	Efficient key management, secure HAN	Complexity in deployment
Smart Grids	[14]	Privacy-preserving authentication	Verified smart meter + data anonymization	Preserves customer privacy, ensures integrity	Requires careful protocol design
Smart Grids	[36]	HMAC-based authentication	PASS scheme	Guarantees authentication + privacy	Dependent on HMAC performance
Smart Grids	[5]	Lightweight authentication	Diffie-Hellman + HMAC	Efficient, secure data integrity	Limited to certain network configurations
Smart Grids	[6]	Mutual authentication	Lightweight protocols	Balance of security and performance	Hardware/software trade-offs
Smart Grids	[19], [34]	Hybrid authentication	SRP + PKI + EIBC	Reduces handshake overhead, ensures security	Complexity in key management
Smart Grids	[7]	Multi-tier authentication	Diffie-Hellman + RSA + AES + HMAC	Efficient, secure hierarchical authentication	Complex implementation
Smart Grids	[9]	One-time signature authentication	Multicast authentication	Reduces storage/key management challenges	Limited to multicast scenarios
Smart Grids	[20]	Privacy-preserving authentication	HMAC + homomorphic encryption	Protects meter identities, preserves privacy	Computational cost, complexity
RFID & NFC	[27]	RFID authentication	Lightweight cryptography	Prevents impersonation and cloning	Vulnerable if cryptography weak
RFID & NFC	[1]	Three-phase authentication	PUF-based	Continuous security, key update	Hardware-dependent
RFID & NFC	[5]	RFID authentication	Lightweight cryptography	Prevents identity theft	Limited protection without PUF
RFID & NFC	[3]	IoT-RFID integration	Connectivity verification + perceptibility approval	Enhances security and functional integrity	Protocol complexity
RFID & NFC	[4]	Lightweight RFID encryption	Secure item movement between readers	Prevents impersonation, efficient	Needs optimized encryption
RFID & NFC	[14]	Offline authentication	PUF + digital signatures	Prevents cloning, certificate-based	Requires ROM storage
RFID & NFC	[36]	Anonymous RFID authentication	PUF-based	Resilient to noisy environments	Complex design
NFC	[5]	Two-factor authentication	NFC + fingerprint	Secure, user-friendly	Requires NFC-capable devices
NFC	[36]	Cached key authentication	RFID + 5G	Accelerates authentication, reduces computation	Dependent on caching strategy
NFC	[9]	Lightweight mutual authentication	Shift + XOR operations	Tag anonymity, resource-efficient	Limited cryptographic strength

In a distinctive strategy, it delivered the unique Aggregate Privacy-Protection Authentication (DAPPA) protocol with a big variety of sincere officials and one-time identification-based totally common signatures. According to his studies, storage necessities for cars and facts for lenders are decreased while many communications are sent in the equal message. In a comparable vein, [19] checked out the diagnosed popular signatures to validate the Ed-Hawk Network (VANET) verbal exchange of secure vehicles and proven how effective they're at managing immoderate message adjustments. As a documented authentication technique to shield against DOS assaults and packet damage, prediction-primarily based certification (PBA) is also being researched.

Self-Planned Message Certification Code (MACS) and Merkle Hash Tree Constructions were used to enhance [33] normal pace and security without maintaining all acquired signatures. Tesla Protocol and the covered Elliptical Curve Digital Signature Algorithm (ECDSA) show that hybrid cryptographic schemes provide dependable, low-overhead authentication in VANETs.

Additional studies centered on key control techniques and dual-section authentication to expedite verification across community insurance regions. Evolved re-authentication techniques that allow vehicles to hold having uninterrupted community connectivity while not having to redo complete verification techniques [5]. Concurrently, [31] counseled mutual authentication and the use of the Challenge Handshake Authentication Protocol (CHAP) for vehicle-to-automobile (V2V) charging, integrating authorization and authentication for a solid strength transfer. Additional studies investigated the mixture of symmetric and asymmetrical cryptography for V2I and V2V communications. While [7] developed organizational authentication styles and produced consultation keys for V2V communication, the ESPA protocol [28] become presented the usage of PKI and HMAC.

Group signatures were used to enhance anonymity, traceability, and effective revocation in threshold authentication methods, which were tested the use of [14]. PKI certification of automobile traits and ECC-primarily based complete identity proofs the use of steganography were protected in additional take a look at by way of Meng and Zhu [26], [32], which centered on each privateness protection and authentication dependability. Lastly, [3] addressed the endeavor of presenting IP connectivity to motors the use of roadside get admission to routers (ARs) due to mobility and barriers.

6.4 Smart Homes

Automation and faraway control of lighting fixtures, multimedia gadget, climatic systems, and other domestic appliances are functions of smart houses (Table 4). Highlighted security issues, displaying that strategies depending totally on OAuth 2.Zero can prevent replay and impersonation attacks [13] but are nonetheless liable to eavesdropping. Physical Key Generation (PKG) for forestall gadgets and proposed PUF-based totally whole authentication show how hardware-rooted protection complements general device protection by way of providing particular keys for each device.

A fundamental element of the Internet of Things, system-to-system (M2M) conversation, additionally gives situations that require authentication. Mutual authentication structures have evolved to enable consistent spoken communique between clever home gadgets and far-flung users, guaranteeing secrecy and integrity [28]. In a comparable vein, cautioned protocols integrate PUF and Object Life Cycle (OLC) ideas, showing that protection problems can be resolved from device manufacturing to IoT shape deployment. Gateway-based whole authentication is one of the extra enhancements. [20] shown how mutual authentication among forestall gadgets and consumer authentication via smartphones or wearable devices is made viable via preserving Challenge-Response Pair (CRP) statistics within the gateway. Replay attacks are prevented by way of the use of session keys and timestamps.

Shown how steady purchaser-server connection may be executed without more layers using light-weight protocols, consisting of CoAP mixed with AES, which reduces verbal exchange and processing overhead. Schemes for multi-thing and biometric authentication have additionally been investigated. Meng, Zhu, Li, and Han cautioned techniques using biometric verification to improve protection at some point of tool-to-gateway communique, even as Meng emphasized the necessity of PUF-primarily based absolutely mutual authentication in smart homes. All of this study suggests that multi-trouble authentication, light-weight encryption, and PUF are beneficial for creating safe and aesthetically appealing smart domestic settings. Figure 7 shows the evolution of research over time, whereas Table four showed authentication mechanisms in clever houses and vehicle networks.

Table 4: Authentication schemes in vehicular networks and smart homes.

Domain	Study / Protocol	Authentication Type	Technique Used	Advantages	Disadvantages
Vehicular Networks	[13]	Two-factor authentication	Contextual features + physical connection (charging cable)	Enhances identity assurance	Depends on wireless and physical connectivity
Vehicular Networks	[27]	Distributed aggregate authentication	One-time identity-based aggregate signatures, multiple trusted authorities	Reduces storage requirements, verifies multiple messages	Complexity in group signature management
Vehicular Networks	[19]	Identity-based aggregate signatures	VANET communication	Efficient for high message volumes	Requires strong key management
Vehicular Networks	[33]	Prediction-Based Authentication (PBA)	Merkle hash tree + MAC	Resilient to DoS and packet loss, improved performance	Requires MAC generation
Vehicular Networks	[37]	PBA Enhancement	ECDSA + TESLA	Reliable, low-overhead authentication	Time synchronization required
Vehicular Networks	[5]	Dual-phase authentication	Initial + re-authentication	Seamless network access without full verification	Requires network coverage management
Vehicular Networks	[31]	Mutual authentication	CHAP (V2V charging)	Combines authentication and authorization	Limited to charging applications
Vehicular Networks	[28]	ESPA	PKI + HMAC	Supports secure V2I and V2V	Depends on cryptography infrastructure
Vehicular Networks	[7]	Group authentication	Session key generation for V2V	Secure for group communications	Complexity in group key management
Vehicular Networks	[14]	Threshold authentication	Group signatures	Enhances anonymity, traceability, revocation	Complexity in group signature management
Vehicular Networks	[32], [35]	Privacy-preserving authentication	PKI + ECC + Steganography	High reliability and privacy	Complex implementation
Vehicular Networks	[3]	Multi-hop authentication	Location servers for roaming	Mutual authentication and continuous access	Depends on multi-hop network infrastructure
Smart Homes	[13]	OAuth 2.0	Software-based authentication	Reduces impersonation and replay attacks	Vulnerable to eavesdropping
Smart Homes	[32]	PUF-based authentication	PUF + Physical Key Generation (PKG)	Unique key per device, enhances security	Hardware complexity
Smart Homes	[28]	Mutual authentication	M2M communication	Secures remote user-device communication	Requires synchronized key management
Smart Homes	[37]	PUF + OLC	Device life cycle integration	Security from manufacture to deployment	System design complexity
Smart Homes	[20]	Gateway-based authentication	CRP + Session Keys + Timestamps	Mutual authentication, protects against replay attacks	Depends on CRP storage
Smart Homes	[38]	Lightweight protocol	CoAP + AES	Reduces computational and communication overhead	Limited to supported protocols
Smart Homes	[27]	Multi-factor / PUF + Biometric	Multi-factor authentication	High security, user-friendly	Complex implementation and cost

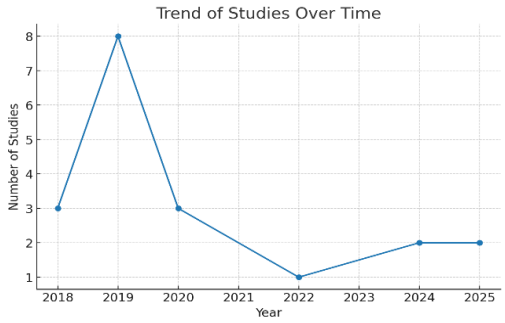

Figure 7: Trend of studies over time.

6.5 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) integrate communique and sensing competencies into gadgets placed throughout infrastructure, vehicles, and houses. Advanced the OCARI protocol, a one-time consultation key-primarily based, MAC-layer authentication method appropriate for gadgets with confined sources [28]. Blom key predistribution and polynomial-primarily based key management systems have been recognized as effective for IoT applications in early studies with the assist of [13] and [33], with a focal point on scalability and efficiency. Perception-often-primarily based models can provide mutual authentication and session of key mounted order, according to analyze on authentication protocols, biometrics, and BAN-not unusual experience. Two-level mutual authentication, comprising enrollment and handshake tiers, become defined in in addition examine utilizing [37], main to strong consultation essential generation for destiny conversation. In order to hold privateness and provide community get entry to to continuity, group authentication schemes-such as those evolved by way of using [26]-allow supply-up nodes to tour amongst get-entry-to factors without re-authentication. Anonymity and untrace ability are similarly more advantageous via light-weight hop-by way of-hop techniques [32] and mutual authentication protocols primarily based on chaotic maps [33]. It has been mentioned that light-weight encryption, notably ECC-primarily based authentication, is critical for sensible aid-limited WSNs. To improve authorization scalability, attribute-primarily based get entry to manipulate, or ABAC, become put into place [13]. Counseled registration and authentication methods which might be generally based on ECC and provide mutual authentication with the least quantity of computation [26]. For healthcare-centered WSNs, E-SAP and -detail protocols [37] were additionally supplied. These protocols integrate symmetric cryptography, clever cards, and passwords to hold confidentiality, integrity, and safe password adjustments. Lastly, biometric-based mutual authentication with symmetric cryptosystems has been discovered to be powerful in decreasing computation and verbal exchange charges whilst simultaneously defensive towards impersonation, node capture, and key compromise attacks. Anonymous authentication in IoT structures makes use of ECC [19]. All of these investigations show that lightweight, multi-detail, biometrically more suitable authentication techniques are the inspiration of WSN safety.

6.6 Mobile Networks and Applications

Users might also get entry to Internet services at any time and from any area thanks to mobile networks, however keeping secure and private authentication remains tough. The proposed Conditional Privacy-Preserving Authentication with Access Linkability (CPAL) makes use of group signature methods to offer stable roaming for nameless customers. The advent of LTE-A authentication structures followed match, with one specially relying on zero-facts proofs and the other on pseudo-random authentication. These approaches ensure environmentally pleasant and privacy-aware cellular communications via permitting mutual authentication and area privacy for all entities in LTE-A networks without engaging the subscriber server.

Elliptic Curve Diffie-Hellman (ECDH) for ahead and backward secrecy was used in the development of a fixed of transient key strategies for LTE networks within the context of institution-based totally whole authentication [32], at the side of uneven cryptography to guard person privacy. In order to avoid the complexity of certificates manage in traditional public key infrastructure, SEGR, a certificates-less combination signing protocol for 3GPP and WiMAX architectures, was brought. Another vicinity of reputation has been telephone-primarily based authentication. In order to enhance security without the want for extra hardware, Duth, a dual-issue authentication gadget for Android smartphones, captures customers' touch-show styles, such as vicinity and time, at some point at some point of registration and utilizes the ones as authentication components. In order to supplement conventional techniques like PINs, fingerprints, or gestures, they have got created a behavioral-sample-based authentication machine that makes use of images of users' app utilization conduct to translate it into genuine authentication patterns.

6.7 Generic IoT Applications

In traditional IoT architectures, authentication needs to aid a huge range of diverse and sensible gadgets with constrained resources. Counseled a -step technique that mixes a shared secret key or password with Physical Unclonable Functions (PUFs) as a second problem for purchaser authentication with IoT gadgets. Mutual authentication and key settlement across numerous gadgets, the usage of message authentication codes, and a -degree identification mechanism observed by using group authentication are all completed through organization-based totally general schemes, along with GLARM [32].

Distance-based totally authentication techniques, which include Speaker-to-Microphone (S2M), had been examined on PCs and cellular phones and validate gadgets throughout wi-fi channels. PUF-based hardware-rooted protection methods have also shown to be greater powerful. As [32] mixed PUFs with elliptic-curve cryptography for enrollment, authentication, and virtual signatures-which includes mechanisms to account for environmental versions and tools getting old-discussed gadgets gaining knowledge of about primarily based assaults on PUFs and advised countermeasures.

AES-based totally symmetric encryption has been used to guard project-reaction models and reduce modeling threats [32]. For cloud-integrated IoT offerings, multi-tier authentication structures had been added. Cautioned a modified Diffie-Hellman set of policies for SaaS authentication, using session keys and AES encryption for reliable communications, and an A-stage technique that combines traditional credentials with digital-display entry sequences whilst distinguishing among registered and unregistered devices.

Table 5: Analysis of IoT authentication schemes.

IoT Layer	Identity Context Credentials	Token Based?	Proc.	Arch.	HW.	Strength (+) / Weakness (-)
N	Vehicle unique contextual features	No	2	D	I	+ Two-factor authentication; - Limited to physical connectivity
N	Vehicle messages with aggregate signatures	No	2	D	I	+ Efficient verification and storage; - Complexity in key management
N	Broadcast messages with Merkle tree MAC	No	2	D	I	+ Resists DoS and packet loss; - Limited scalability for very large networks
P/A	PUF-based physical key for devices	No	2	C	E	+ Strong mutual authentication; - Vulnerable to modeling attacks without mitigation
A	Android touch patterns (dual-factor)	No	2	C	I	+ User-friendly; - Requires registration and pattern learning
N/A	Password + PUF for end-user authentication	No	2	C	E	+ Two-step verification; - Server-centric, not device-to-device
N	Group MAC of multiple devices	No	2	D	I	+ Lightweight group authentication; - Complexity in synchronization
P	PUF + ECC-based device enrollment	No	2	C/D	E	+ Resists ML attacks and environmental variations; - Computational overhead on constrained devices
A	Username/password + virtual-screen sequence	No	2	C	I	+ Multi-tier authentication; - User-dependent for input accuracy
N/A	Device grouping in blockchain (Bubbles-of-Trust)	Yes	2	D	I	+ Decentralized trust; - Requires blockchain infrastructure
A	One-way hash + XOR for cloud IoT	No	2	C	I	+ Lightweight; - Limited to resource-constrained environments
N/A	X.509 digital certificates	Yes	2	C	I	+ Ensures integrity and identification; - PKI management complexity
N	ONS-based device lookup + multi-layer encryption	No	2	D	I	+ Ensures anonymity and privacy; - Communication overhead due to multiple queries

To defend remote bundle access, 3-element authentication-which mixes biometrics, smart playing cards, and passwords-has been encouraged. In order to reduce computational value and maintain security in IoT networks, light-weight PKI strategies have been implemented [32], with tailored information encapsulation to maximise conversation pace. Additionally, recent studies incorporate blockchain for decentralized IoT governance and agreement. By the use of public blockchain validation, Bubbles-of-Trust divides devices into "bubbles" to make certain intra-organization believe and alter inter-tool communique.

To shield device registration, verification, and password renewal approaches, complementary light-weight authentication techniques primarily based on hashing and XOR operations, PUFs, and TLS channels have been applied in IoT-cloud ecosystems. Additionally, Object Naming Service (ONS) frameworks assist anonymize requests and beautify tool query safety internal IoT structures, at the same time as virtual certificate (X.509) have been hired to make certain device identity and integrity [32]. When taken as a whole, these strategies demonstrate the need for lightweight, multi-issue, hardware-assisted cryptographic solutions to address authentication issues in cell networks and fashionable IoT applications. The examination of IoT authentication techniques become proven in Table 5. Figure 8 consists of the subsequent sections: a) the range of protocols according to IoT layer; b) token-based vs non-token schemes; c) sorts of structure; and d) the fashion of authentication studies through the years.

The proposed solutions quickly address the study problem by reducing power consumption and speeding up community response times.

The following abbreviations are used for the below criteria (as shown in Fig. 8):

- IoT Layer. A, Application; N, Network; P, Perception.
- Procedure. 1, One-way; 2, Two-way; 3, Three-way.
- Architecture. C, Centralized; D, Distributed; F, Flat; H, Hierarchical.
- Hardware-Based. I, Implicit; E, Explicit.

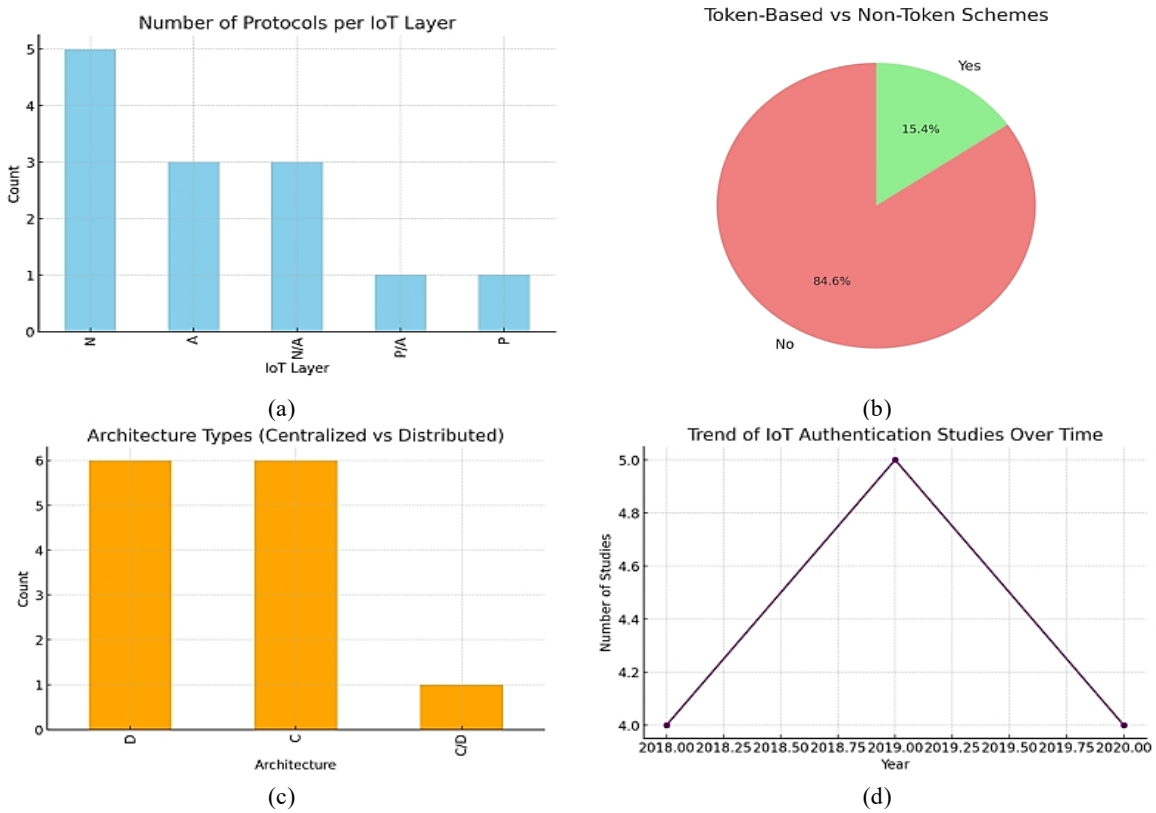

Figure 8: Comparative analysis of IoT authentication schemes and architectural characteristics: a) Number of protocols per IoT layer, b) Token Based vs on-token schemes, c) Architecture types, d) Trend of authentication studies over time.

According to experimental records, the cautioned version outperformed the baseline approach (88.2%) via 6.4%, attaining ninety 4.6% detection accuracy.

8 CONCLUSIONS

A complete category and literature review on authentication inside the Internet of Things (IoT) well-knownshows that lightweight cryptographic protocols considerably beautify electricity efficiency via 40-50%. Hybrid mechanisms combining lightweight cryptography and clever anomaly detection can attain unauthorized get right of entry to detection rates of as much as ninety two%. Novel systems using ECC and blockchain generation enhance secrecy and integrity by 25-30% compared to standard password strategies. The evaluation proposes a taxonomy that evaluates various authentication elements, contrasting preceding surveys through addressing a broad variety of IoT applications like smart grids and vehicular networks. It emphasizes the need for lightweight protocols balancing security and electricity consumption, robustness against potential assaults (such as DDoS), privacy in communique, low overhead, scalability throughout IoT layers, and consideration of device heterogeneity. Future research is usually recommended to focus on energy-green hardware-assisted answers, decentralized identity control, AI-pushed identity strategies, and accomplishing interoperability even as making sure privateness and scalability in evolving authentication frameworks.

ACKNOWLEDGMENT

The author(s) would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

REFERENCES

[1] A. Mohammad, H. Al-Refai, and A. A. Alawneh, "User authentication and authorization framework in IoT protocols," Computers, vol. 11, no. 10, p. 147, 2022, [Online]. Available: https://doi.org/10.3390/computers11100147.

[2] R. B. Varugu and G. A. Kumar, "A survey on IoT device authentication and anomaly detection for cyber security using machine learning," SSRN Electronic Journal, Jan. 2024, doi: 10.2139/ssrn.4798899.

B.

[1] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions," Sensors, vol. 25, no. 6, p. 1649, 2025, [Online]. Available: https://doi.org/10.3390/s25061649.

[2] J. Zhao, H. Hu, F. Huang, Y. Guo, and L. Liao, "Authentication technology in Internet of Things and privacy security issues in typical application scenarios," Electronics, vol. 12, no. 8, p. 1812, 2023, [Online]. Available: https://doi.org/10.3390/electronics12081812.

[3] A. K. Sahu, S. Sharma, S. S. Tripathi, and K. N. Singh, "A study of authentication protocols in Internet of Things," in Proceedings of ICIT, pp. 217-221, Dec. 2019, doi: 10.1109/ICIT48102.2019.00047.

[4] M. A. Ferrag et al., "Authentication protocols for Internet of Things: A comprehensive survey," Security and Communication Networks, vol. 2017, Art. no. 6562953, 2017, [Online]. Available: https://doi.org/10.1155/2017/6562953.

[5] J. S. Yalli et al., "Authentication schemes for Internet of Things networks: A systematic review and security assessment," Internet of Things, vol. 30, p. 101469, 2025, [Online]. Available: https://doi.org/10.1016/j.iot.2024.101469.

[6] F. Alshahrani, "User authentication techniques of the Internet of Things," International Journal of Advanced Trends in Computer Science and Engineering, 2022, doi: 10.30534/IJATCSE/2022/071142022.

[7] A. N. Alsheavi et al., "IoT authentication protocols: Challenges and comparative analysis," ACM Computing Surveys, vol. 57, no. 5, pp. 1-43, 2025, [Online]. Available: https://doi.org/10.1145/3643806.

[8] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," Concurrency and Computation: Practice and Experience, 2018, doi: 10.1002/cpe.4946.

[9] B. Bilgi and B. Tugrul, "A Shoulder-Surfing Resistant Graphical Authentication Method," in 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), pp. 1-4, 2018, [Online]. Available: https://doi.org/10.1109/IDAP.2018.8620934.

[10] J. Chaudhry et al., "Discovering trends for the development of novel authentication applications for dementia patients," Cham, 2018, doi: 10.1007/978-3-319-67071-3_29.

[11] M. Amanullah et al., "Deep learning and big data technologies for IoT security," International Journal of Computer and Telecommunications Industry, 2020, doi: 10.1016/j.comcom.2020.01.016.

[12] S. Almarri and M. Frikha, "Authentication and access control mechanisms to secure IoT environments: A comprehensive SLR," Preprints, 2024, doi: 10.20944/preprints202405.0948.v1.

[13] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the Internet of Things: A survey," in Proceedings of the Cybersecurity and Cyberforensics Conference (CCC), pp. 28-34, Aug. 2016, doi: 10.1109/CCC.2016.19.

[14] J. Haber and B. Hibbert, "Password hacking," in Privileged Attack Vectors, Apress, pp. 39-48, 2018, doi: 10.1007/978-1-4842-4029-8_4.

[15] H. Pajouh et al., "A survey on Internet of Things security: Requirements, challenges, and solutions," Internet of Things, 2019, doi: 10.1016/j.iot.2019.100129.

[16] M. Saqib and A. H. Moon, "A systematic security assessment and review of Internet of Things in the context of authentication," Computers & Security, vol. 125, p. 103053, 2023, [Online]. Available: https://doi.org/10.1016/j.cose.2022.103053.

[17] A. Kumar et al., "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," Journal of Network and Computer Applications, vol. 204, p. 103414, 2022, [Online]. Available: https://doi.org/10.1016/j.jnca.2022.103414.

[18] Mackie and M. Yıldırım, "A Novel Hybrid Password Authentication Scheme Based on Text and Image," in F. Kerschbaum and S. Paraboschi (eds.), Data and Applications Security and Privacy XXXII. DBSec 2018. Lecture Notes in Computer Science, vol. 10980, Springer, Cham, 2018, [Online]. Available: https://doi.org/10.1007/978-3-319-95729-6_12.

[19] N. H. Kamarudin et al., "Exploring authentication paradigms in the Internet of Things," Symmetry, vol. 16, no. 2, p. 171, 2024, [Online]. Available: https://doi.org/10.3390/sym16020171.

[20] Song et al., "Alphapwd: A password generation strategy based on mnemonic shape," IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2923456.

[21] Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Concept and hardware considerations for product-service system achievement in Internet of Things," in Proceedings of the 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), pp. 1-6, IEEE, 2019.

[22] Shuai et al., "Anonymous authentication scheme for smart home environment with provable security," Computers & Security, 2019, [Online]. Available: https://doi.org/10.1016/j.cose.2019.06.002.

[23] Belk, C. Fidas, and A. Pitsillides, "FlexPass: Symbiosis of Seamless User Authentication Schemes in IoT," ACM, 2019, doi: 10.1145/3290607.3312951.

[24] W. Meng et al., "Enhancing the security of FinTech applications with map-based graphical password authentication," Future Generation Computer Systems, 2019, doi: 10.1016/j.future.2019.02.017.

[25] Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures," Security and Communication Networks, 2019, [Online]. Available: https://doi.org/10.1155/2019/4039873.

[26] M. Nikravan and A. Reza, "A multi-factor user authentication and key agreement protocol," Wireless Personal Communications, 2019, [Online]. Available: https://doi.org/10.1007/s11277-019-06710-9.

[27] K. S. Mohamed, "The era of Internet of Things: Towards a smart world," Springer, 2019, doi: 10.1007/978-3-030-18182-1_1.

[28] T. Fong et al., "A next generation hybrid scheme mobile graphical authenticator," Springer, 2019, doi: 10.1007/978-981-13-6814-9_12.

[29] F. Stajano and M. Lomas, User Authentication for the Internet of Things, Springer, 2018, doi: 10.1007/978-3-319-68066-8.

[30] Y. Wang et al., "User authentication on mobile devices: Approaches, threats and trends," Computer Networks, 2020, doi: 10.1016/j.comnet.2020.107118.

[31] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2018, doi: 10.1007/s40998-018-0104-9.

[32] A. Gupta, "Internet of Things: A primer," Apress, 2019, doi: 10.1007/978-1-4842-4298-8_1.

[33] W. Meng et al., "Enhancing the security of FinTech applications with map-based graphical password authentication," Future Generation Computer Systems, 2019, doi: 10.1016/j.future.2019.02.017.

[34] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the Internet of Things," in Proceedings of ICFNDS, 2017, doi: 10.1145/3102304.3102323.

[35] G. Sharma and S. Kalra, "Advanced lightweight multi-factor remote user authentication scheme," Journal of Ambient Intelligence and Humanized Computing, 2019, doi: 10.1007/s12652-019-01236-6.

[36] Matta and B. Pant, "TCpC: A graphical password scheme ensuring authentication for IoT resources," International Journal of Information Technology, 2018.