Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.048796

REVIEW

Recent Developments in Authentication Schemes Used in Machine-Type Communication Devices in Machine-to-Machine Communication: Issues and Challenges

Shafi Ullah[1], Sibghat Ullah Bazai[1,*], Mohammad Imran[2], Qazi Mudassar Ilyas[3,*], Abid Mehmood[4], Muhammad Asim Saleem[5], Muhmmad Aasim Rafique[3], Arsalan Haider[6], Ilyas Khan[7], Sajid Iqbal[3], Yonis Gulzar[4] and Kauser Hameed[3]

[1]Department of Computer Engineering, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta, 87300, Pakistan

[2]Department of Information Technology, Balochistan University of Information Technology, Engineering, and Management Sciences, Quetta, 87300, Pakistan

[3]Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Hofuf in Al-Ahsa, 31982, Saudi Arabia

[4]Department of Management Information Systems, College of Business Administration, King Faisal University, Hofuf in Al-Ahsa, 31982, Saudi Arabia

[5]Department of Software Engineering, College of Computing, Riphah International University, Faisalabad, 44000, Pakistan

[6]Department of Electrical Engineering Balochistan University of Information Technology, Engineering, and Management Sciences, Quetta, 87300, Pakistan

[7]Department of Mathematics, College of Science Al-Zulfi, Majmaah University, Al-Majmaah, 11952, Saudi Arabia

*Corresponding Authors: Sibghat Ullah Bazai. Email: sibghat.ullah@buitms.edu.pk; Qazi Mudassar Ilyas. Email: qilyas@kfu.edu.sa

Received: 19 December 2023 Accepted: 14 February 2024 Published: 25 April 2024

ABSTRACT

Machine-to-machine (M2M) communication plays a fundamental role in autonomous IoT (Internet of Things)-based infrastructure, a vital part of the fourth industrial revolution. Machine-type communication devices (MTCDs) regularly share extensive data without human intervention while making all types of decisions. These decisions may involve controlling sensitive ventilation systems maintaining uniform temperature, live heartbeat monitoring, and several different alert systems. Many of these devices simultaneously share data to form an automated system. The data shared between machine-type communication devices (MTCDs) is prone to risk due to limited computational power, internal memory, and energy capacity. Therefore, securing the data and devices becomes challenging due to factors such as dynamic operational environments, remoteness, harsh conditions, and areas where human physical access is difficult. One of the crucial parts of securing MTCDs and data is authentication, where each device must be verified before data transmission. Several M2M authentication schemes have been proposed in the literature, however, the literature lacks a comprehensive overview of current M2M authentication techniques and the challenges associated with them. To utilize a suitable authentication scheme for specific scenarios, it is important to understand the challenges associated with it. Therefore, this article fills this gap by reviewing the state-of-the-art research on authentication schemes in MTCDs specifically concerning application categories, security provisions, and performance efficiency.

KEYWORDS

Authentication; cyber security; internet of things; machine-type communication devices; machine-to-machine communication

1 Introduction

Internet usage has become an indispensable part of routine life. It has become integral in every facet of human lives, whether directly or indirectly, encompassing finance, education, healthcare, and social interactions. As of 2023, the global count of internet users has reached 5.18 billion, which indicates that approximately two-thirds of the world's population is presently linked to the World Wide Web [1,2]. Besides, the world of automation has also created a surge. It has not only enabled humans to communicate over the Internet but also enabled machines to communicate with each other through M2M (machine-to-machine) and MTCDs (machine-type communication devices) technologies where human intervention is no longer a mandate. It is estimated that by 2025, over fifty billion devices will be employed in the cause. Compact and well-designed equipment, also known as MTC (machine-type communication) devices, are handed down in everyone's life, ranging from smart refrigerators, televisions, and air-conditioner controllers to smart health devices, smart offices, and smart parking. These devices serve multiple functions, such as monitoring air quality in homes, sensing the environment in cities, granting access to authorized personnel in the office via smart doors, regulating specific machines controlled by the ventilation system, and tracking vital signs like heart rate and body temperature, transmitting this health data to physicians, securing parking spots in advance on busy streets, and generating environmental data for informed decision-making and future predictions. These devices utilize internet connectivity to share data and execute tasks based on pre-programmed logic. Despite their small size, cost-effectiveness, and limited computational abilities, these diminutive yet intelligent devices communicate, exchanging information as depicted in Fig. 1.

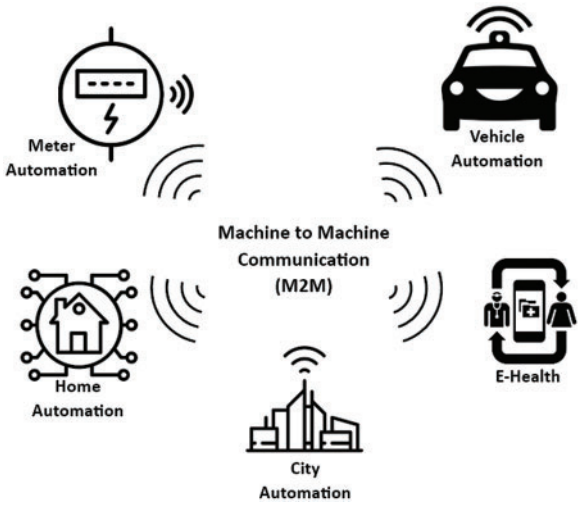

Figure 1: M2M communication applications

The information exchanged by these MTCs can range from public data to overly sensitive information. For instance, a device might share temperature data from a power station to regulate fans, while another might transmit a remote heart patient's heartbeat data to their doctor. Similarly, life-threatening dangers can arise from hacking into medical device MTCDs. In smart grids, unauthorized access can potentially interfere with electricity distribution and cause blackouts. In the case of industrial IoT (Internet of Things) networks, unauthorized access can impact safety and manufacturing operations. In the context of smart homes, unauthorized control of IoT devices threatens the privacy and security of residents [1]. Similarly, certain devices control access to secure military facilities. In these scenarios, the shared data is exceptionally sensitive. However, as MTCDs lack inherent security measures, external physical safeguards are not always feasible since these devices are meant to function remotely and autonomously.

Moreover, securing data and devices becomes challenging due to various factors, including limited connectivity, harsh environmental conditions, restricted physical access, power constraints, and limited maintenance opportunities. MTCDs deployed in remote locations often suffer from brittle network connectivity, which may compromise real-time communication with security infrastructure. As a result, security updates, patches, and monitoring activities are delayed, which increases devices' vulnerability to emerging security threats. Harsh environmental conditions, temperature variations, and exposure to dust or moisture harm the physical integrity of MTCDs, which causes hardware degradation and compromises the device's ability to enforce security measures. Restricted physical access to MTCDs makes physical security measures challenging to implement. It also raises concerns about unauthorized access, tampering, or theft of devices. MTCDs deployed in remote environments usually lack reliable power sources and rely on batteries. Insufficient power can lead to unexpected device shutdowns, leaving systems unprotected during critical times. Finally, there are limited maintenance and update opportunities for MTCDs in remote or harsh environments, which results in outdated firmware or security protocols that may expose devices to known vulnerabilities.

The threats mentioned above may be mitigated by carefully implementing device, data, and user authentication mechanisms. A robust device authentication mechanism involves a secure device provisioning through device identity verification during device enrollment on the network, a mutual authentication mechanism to enforce mutual authentication between devices and network servers, and multi-factor authentication by requiring multiple credentials, e.g., digital certificates, hardware tokens, or passwords for device access. Data authentication can be implemented through digital signatures, message authentication codes, and hash functions. User authentication can be implemented through strong password policies, role-based access control, and biometric authentication.

Consequently, these devices rely solely on software-based security measures. Owing to their limited computational and memory capacities, conventional Internet security protocols do not always apply to these IoTs [3]. Effectively operating MTC communication necessitates a network of MTC-based devices. This network may, in turn, consist of several connected devices, and every device must be trusted to ensure security. This is achieved via authentication, where every device in the network must authenticate itself so that the data is considered trusted.

This review is based on authentication techniques proposed in different applications for securing MTC devices under the IoT (Internet of Things) framework. This article represents a thorough review of the authentication of MTC devices in M2M (machine-to-machine) communication in three categories, i.e., *local*, *group*, and *factor-based* authentication techniques, where several related techniques are analyzed regarding performance efficiency, security, and adaptability.

1.1 Contribution of Research

This work offers a thorough idea to the researcher related to the perceptual layer security requirements and features in M2M communication networks, as MTC devices are best suited for efficient performance in the perceptual layer. Moreover, the work categorizes authentication schemes into three categories and compares different authentication schemes. Furthermore, the authentication taxonomy in the last section offers a thorough understanding of authentication features and processes in the recent IoT security developments.

The paper is organized in the following manner. Section 2 represents Authentication in MTC devices, including perception layer security threats and requirements. Section 3 offers comparative analysis features adopted to analyze the categorized authentication schemes in the M2M communication network. Section 3 highlights issues and challenges. The paper is concluded in Section 5.

2 Machine-Type Communication Devices

MTC devices are autonomous IoT devices whose core functionality is to operate in remote areas in M2M communication networks. These devices are mostly battery-powered that collect, process, and transmit data to central nodes or gateways to be stored on the cloud for further processes [4].

2.1 MTC Device Layers

The functions of these devices are distributed in four layers, as summarized in Table 1.

Table 1: Generic four-layer architecture of IoT

Layers	Name	Function	Devices/Applications
Layer 4 [5]	Application layer	• Representation of collected and processed data into a pre-defined graphical interface. • To automate and make smart decisions by the device. • Smart IoT business applications.	• Smart home automation system • Smart healthcare system • Smart industry
Layer 3 [6]	Middle-ware layer	• Data management functions. • Automate the flow of tasks based on received information from the perception or network layer. • Inclusion of database-related actions for storage.	• Software-based • Built-in circuitry
Layer 2 [7]	Network layer	• Data generated from sensors is converted into packets to match standard protocol patterns. • Forwarding data packets to 3G, LTE structured packets in wire/wireless medium.	• Utilizing standard communication equipment • Software-based • Built-in circuitry

(Continued)

Table 1 (continued)

Layers	Name	Function	Devices/Applications
Layer 1 [8]	Perception layer	• Data generation layer, sensing environmental data from sensors and actuators and converting it to digital information. • These sensors collect data and send it to MTC devices, which are further processed for transmission.	• Temperature, pressure, humidity, and heartbeat sensors • RFID, barcode readers • ZigBee, Bluetooth

2.2 Security Features in the Perception Layer of MTC Devices

Research offered by [4] and [9] shows that the perceptual layer security can be separated into two categories, i.e., security and technological challenges. The technological category focuses on challenges due to the dynamic topologies of MTC devices and the ubiquitous behavior of IoT and M2M network applications. It includes areas such as energy, power, distributed features, and risks. Whereas, security challenges primarily aim to address solutions and weaknesses in end-to-end encryption, data integrity, data confidentiality, and scalability to ensure authentication between these devices [9]. Moreover, the authentication scheme is chosen considering the nature of communication within the network and the type of business application required, and with certain cryptosystem techniques.

Table 2 represents perceptual layer security features for MTC devices in the M2M communication network. Each perceptual layer security feature enhances resilience against the perceptual layer security threats, as shown in Table 3. The represented authentication schemes are tested for performance efficiency and verified for security proofs against several features, as shown in Table 4.

Table 2: Perception layer security features in M2M communication

	Features	Description	Ref.
BASIC	Data integrity	Data integrity is the accuracy of data shared between devices. It ensures that data from the sender device is trusted, accurate, and clean from intended or unintended interference, usually made possible by imposing end-to-end encryption.	[10]
	Privacy	Privacy of shared sensitive data is paramount. The sensitivity of data mainly depends on the type of IoT application. It refers to both the confidentiality of data and the privacy of the device that shares it.	[3]

(Continued)

Table 2 (continued)

	Features	Description	Ref.
	Authentication	It is a key security feature because communication between numerous devices of heterogeneous nature makes it vital for the data sender to be trusted. During authentication, all participating devices in the communication must be authenticated to establish trust.	[11]
	Data availability	It serves devices with a constant flow of data whenever data is required. The main purpose of MTC devices is to operate all the time under any circumstances with minimal cost, even during times of failure, despite the system facing a disastrous situation.	[12]
	Data confidentiality	Data transmitted from a device is not only kept secret from other users but from neighboring devices as well. It is maintained by combining features of authentication and integrity, where authentication establishes trust between devices (operated by either user or device), and integrity ensures the shared data is reliable.	[13]
	Access control	It manipulates access of MTC devices to back-end servers during requested access. Only authorized devices can be granted access to certain entities, including servers and other crucial devices.	[14]
ADVANCED	Data freshness	Data freshness ensures that only currently transmitted messages from MTC devices are received. Previously transmitted messages are discarded and cannot be read by newly added devices or devices that have left the system.	[15]
	Data secrecy	Data secrecy focuses on message security from newly joined MTC devices or devices that have left the network. Each message header represents a new encrypted key that can only be decrypted or decoded by current devices.	[15]
	Forward secrecy	It ensures that encrypted keys cannot be compromised, and long-term secrets can be kept despite adding more devices and users.	[15]
	Backward secrecy	It assures that the adversary who knows a subset of keys cannot discover the previous keys despite adding and removing new and old devices.	[16]
	Non-repudiation	It improves message delivery by not denying message packets once MTC devices transmit them.	[15]

(Continued)

Table 2 (continued)

	Features	Description	Ref.
	Collision detection	It is a combination of several inputs that produce the same hash value. It must be kept highly random and challenging to acquire a proper set of these inputs.	[17]

Table 3: Perception layer security attacks in M2M communication devices

Attacks	Description	Ref.
Trojan hardware	It is an integrated circuity fabricated attack to influence the data by attaching a fictitious IC on a device to exploit functionality. Attackers use such ICs to copy ongoing shared data for a certain period.	[18,19]
Non-network side channel	The wireless signals generate electromagnetic waves that transmit critical data. Researchers demonstrated acoustic, electromagnetic signals leaking from an isolated MTC device that released sensitive information, resulting in data privacy and confidentially vulnerabilities.	[20]
DoS	Such attacks on IoTs and MTC devices stop functionality by transmitting sensors' HIGH/LOW-status signals to keep the device occupied. It further aims to deplete the device from power and sleep to waste power and energy.	[21]
Power depletion	MTC devices are mostly attached to external batteries with limited energy due to mobility. These Devices consume energy during operation; otherwise, devices go into standby mode to reduce power usage. DoS power depletion attacks aim to send consecutively fake data via sensing circuitry so that devices are kept on consuming power. For example, the device's battery life is so depleted that it cannot work or report in crisis.	[22,23]
Sleep deprivation	Such an attack bars the device from going into sleep mode by posting undesired requests of HIGH states. The adversary attempts to send bogus signals that are genuine.	[23,24]
Malfunction	It is an effect of an accidental or intended blunder during sleep deprivation, hardware assembly, code infusion, or power depletion.	[25]
Outage/blackout attack	Devices suffer blackouts by halting the execution of their typical task. A master MTC device regulates several slave sensing and actuating devices. Thus, if the master device halts functionality, the attached slave devices are also affected.	[26]

(Continued)

Table 3 (continued)

Attacks	Description	Ref.
Physical attack	MTC devices are exceptionally vulnerable to physical attacks due to the remote operational ability where human intervention is undesired. The adversary's physical access can extract crucial data, penetrate internal circuitry, modify data transmission lines, and alter functional tasks.	[27]
Device capture/replication	The adversary captures and replicates with a malicious device, which then intrudes into the network by imitating genuine device features. The attacker will be able to redirect packets to the desired network and can cause damage to the network by discovering pre-shared keys.	[28,29]
Sensor capture	Sensor capture may result in a DoS attack. Such an attack occurs when the attacker attempts to misguide and manipulate control over the sensor-driven functions.	[29]
Disguised device	The attacker embeds a fake device or attacks an approved device to cover up at the perception level to store critical data in the flow and divert the traffic.	[29,30]
Infusing malicious device	A fraudulent device is connected to the network that produces fake and illegitimate requests and attempts to obtain access to neighboring devices. It also attempts to virtually control the system or neighboring devices via the infused malicious code.	[30]
Eavesdropping	It is the most lethal attack in IoT. Deprived of any significant data encrypting protocol, typical security protocols in MTC devices cannot hide data from such attacks. Eavesdropping is when transmitted data over physical lines of communication is monitored by another device.	[31]
MiTM	A device monitors the traffic forcibly connected between sender and receiver, and both transmitting and receiving devices have no clue that the communication is being monitored. The monitored data is read thoroughly, interpreted, and decrypted.	[32]
Spoofing	The transmitting data is monitored briefly, capturing sufficient packets to be interpreted, make sense of the data, and then combined with malicious packets that mimic genuine packets. It is applied on physical transmitting devices over both wired and wireless media.	[31]
Routing attacks/sybil	Routing protocols that redirect the traffic are targeted during such attacks. A malicious device generates duplicate nodes in the network that redirect traffic to affect performance.	[33]
Wormhole	It is a combined attack of Spoofing and Sybil. The attacker stores packets over time, interprets the packet, and then redirects the recorded packets to other unauthorized networks.	[34]

Table 4: Comparative analysis tools and features used in M2M communication

	Analysis features	Description	Ref.
Performance	Computational cost	CPU time consumed in successful mutual authentication between two devices.	[35,36]
	Communication cost	Time taken in transmitting and receiving packets during a successful mutual authentication process.	[10]
	Energy cost	Total power consumption (CPU, idle, transmit, and listen power) in a successful mutual authentication process.	[37]
	Storage cost	The total memory consumed (RAM and ROM) in storing pre-shared keys, code size, and heap during a successful mutual authentication process.	[35,36]
Encrypted key exchange	Key sensitivity	Ability to change whole encrypted block in case of a single bit change in (pre-shared, dynamic, static, public, and private) encrypted keys.	[38]
	Randomness	Ability to produce unique and random key pairs/encrypted blocks. It is also measured as the ratio of bit difference before and after the encryption.	[39]
	Key generation cost	Execution Time and memory consumed during the generation of pre-shared, dynamic, public, or private keys.	[40]
	Cross-correlation	There must be tight cross-correlation between key pairs before and after the encryption of keys.	[1]
Verification tools	NIST	The robustness of encrypted blocks is analysed by forcibly cracking and decoding the encryption through several advanced statistical procedures.	[39]
	AVISPA	Mutual authentication processes are verified through tight security communication procedures by visualizing the processes of sender and receiver devices.	[41]
	BAN	Logically evaluates transmission messages and ensures the exchanged data's trustworthiness over the media by verifying data origin, freshness, and reliability.	[42]

(Continued)

Table 4 (continued)

	Analysis features	Description	Ref.
	ProVerif	This tool is used for automated reasoning related to the security properties in formal cryptographic techniques.	[43,44]

3 Authentication in MTC Devices

Authentication is a software-based security technique used in different topologies. MTC devices form three types of authentications in M2M communication, i.e., local, group-based, and hybrid (factor-based). In the local authentication, all devices authenticate within the connected network. Any other device outside the network cannot share the data. In comparison, group-based authentication is used for a large number of devices working in simultaneous prospects of applications. Several devices form a group using local authentication techniques and cluster single groups. These groups authenticate other groups, and data is shared. Such authentication processes usually occur in LTE (long-term evolution)/CDMA (code-division multiple access) and 3GPP (3rd Generation Partnership Project)-based network infrastructures.

Moreover, in hybrid or factor-based authentication, M2M communication occurs between an end device, i.e., MTC, and a gateway, making it two-factor authentication. The process of key sharing, encryption, and decryption is performed for both MTC and gateway. Similarly, three-factor authentication involves servers or clouds as the third tier of communication. In such a technique, servers and gateways must utilize similar distributed encrypted keys for authentication. Additionally, mutual authentication is an important part of authentication where data transmitting and receiving devices must mutually authenticate each other before sharing the actual data.

3.1 Group-Based Authentication

Such authentication protocols are used when a network consists of a large number of MTC devices. Single-device authentication is costly, and it includes extreme network overheads. Moreover, the area coverage is extremely large. Thus, numerous devices communicate simultaneously, so group-based authentication is effective against network overheads [45]. Standard encryption systems use either symmetric, asymmetric, or hybrid cryptographies. With extreme growth in wireless sensor networks [4], MTC devices are also introduced in LTE-A (long-term evolution-Advanced) networks, implementing 4G heterogeneous networks with low latency. LTE/LET-A networks tend to have a pre-defined authentication system between communication units for MTC network architecture, which was introduced by the 3GPP committee [2]. The network comprises MME (mobile management entity) and HSS (home subscriber server). The architecture includes users or MTC devices and servers, whereas the user is outside the network domain. Users or MTC devices and servers communicate over an API (application programmable interface), as shown in Fig. 2. Users or MTC devices must authenticate over the LTE/LTE-A network. In this regard, the EPS-AKA (evolved packet system-based authentication and key agreement) developed a packet delivery system for the 3GPP network with an extended version called EAP-AKA (extensible authentication protocol-authentication and key agreement) for the non-3GPP network over WLAN (wireless local area network)/WiMAX (worldwide interoperability for microwave access) was implemented for the objective of secure data transfer between MTC devices and server [46].

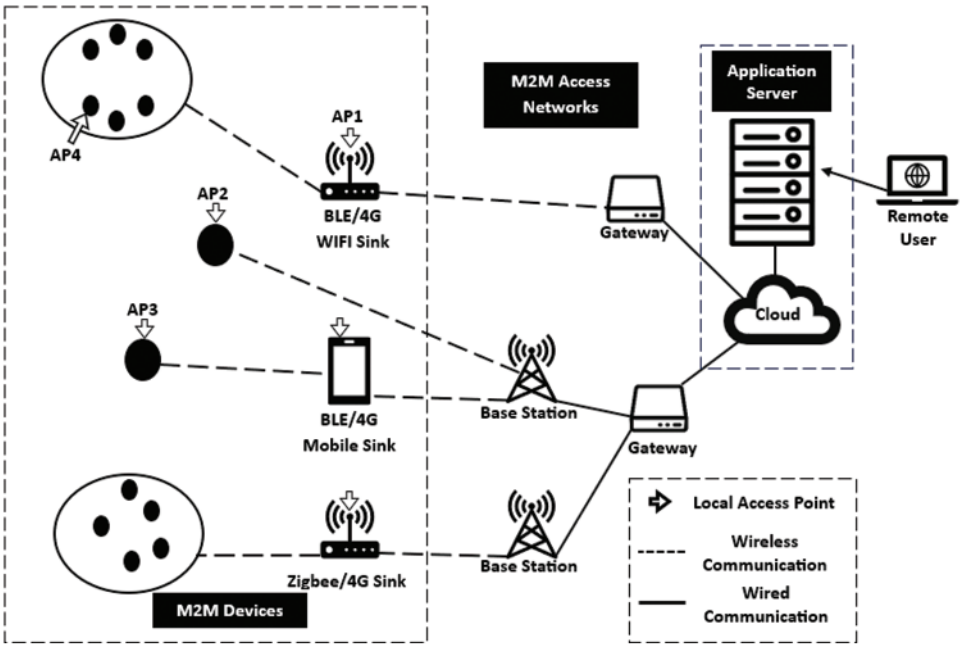

Figure 2: Local authentication network structure based on [1]

Several key agreeing protocols use the 3GPP network architecture. These protocols improve security and lessen network overheads. Jung et al. [47] devised congestion avoidance to prevent signaling congestion. In extension, Chen et al. [48] applied a similar grouping approach in G-AKA where the initiator device is verified by HSS, which then authorizes the MME entity. Still, it is susceptible to MiTM (man in the middle) and DoS (denial of service) threats. Lai et al. [49] proposed SE-AKA (secure and efficient authentication and key agreement), where a novel asymmetric method of encoding keys was introduced, which later proved less useful *vs.* signaling congestion. Jiang et al. [50] proposed EG-AKA (EAP-based group authentication and key agreement) to validate a local group of MTC devices. Still, the procedure is susceptible to MiTM, DoS, and re-directional threats. The MTC-AKA (machine-type communication authentication and key agreement) by Lai et al. [51] first used fully authenticated MTC devices with HSS, which authenticated reaming MTC devices through a group temporary key—however, the protocol suffered from security attacks. Choi et al. [52] endorsed the GROUP-AKA protocol to alleviate signaling congestion where groups of devices were validated with reduced signaling congestion. Devices could easily join and leave the group but lacked in device privacy preservation. Cao et al. [53] developed GBAAM-AKA (group-based access authentication for MTC-authentication and key agreement) to address the privacy preservation challenge. Moreover, High-level computation overheads were created as GBAAM-AKA followed an asymmetric cryptosystem. Fu et al. [54] introduced the PRIVACY-AKA protocol that creates pseudo-identity via elliptic curve cryptography through group leaders, where the group leaders receive MAC from devices and produce an accumulated MAC. The scheme responds to primary security risk without key secrecy and produces network overheads. Lai et al. [55] recommended GLARM-AKA (group lightweight authentication scheme for resource-constrained M2M-authentication and key agreement), which is lightweight and produces less network signaling overheads in comparison to primitive AKA protocols but it fails due to unlink-capability. The protocol deteriorates from newly joining and old devices leaving the system, which gives a chance to DoS assaults and privacy issues. Li et al. [38] improved GR-AKA's

unlinkability by endorsing a dynamic policy in LTE-A. However, strong cryptography resulted in heavy bandwidth consumption. Yao et al. [56] proposed GBS-AKA (group-based secure authentication and key agreement) and improved overhead and bandwidth consumption but failed to incorporate privacy preservation.

Table 5 shows the group-based techniques that attempt to improve performance and adapt resilience against several security threats. Each work achieves a specific goal but lacks a thorough security-resilient mutual authentication scheme.

Table 5: Summary of discussed group-based authentication schemes

Schemes	Features	Basic security features				Threat vulnerabilities					Performance weaknesses
		S1	S2	S3	S4	T1	T2	T3	T4	T5	
G-AKA [52]	Entity-based mutual authentication	N	N	Y	N	Y	Y	Y	Y	Y	High computational overhead
SE-AKA [49]	Asymmetric cryptosystem	N	Y	Y	Y	Y	Y	N	N	Y	Network signalling congestion
EG-AKA [50]	Non-3gpp network authentication	Y	Y	Y	N	Y	N	Y	Y	Y	Computation overload at the network
MTC-AKA [51]	Entity-based mutual authentication	N	Y	Y	Y	Y	N	N	N	Y	DOS-infused redirection attacks
GBAAM-AKA [53]	Signature-based authentication	N	N	Y	N	N	N	N	Y	Y	High computational overheads
GROUP-AKA [52]	Improved unlink-ability	Y	N	Y	N	N	Y	N	Y	Y	Weak key forward secrecy
GLARM-AKA [55]	Group-bases lightweight cryptography	Y	Y	Y	N	N	N	Y	Y	Y	Weak unlink-ability (both KFS/KBS)
Privacy –AKA [54]	Pseudo-identity via ECC-based mutual authentication	N	Y	Y	Y	N	N	Y	Y	N	Weak key forward secrecy
GR-AKA [38]	Flexible policy by lagrange component (LC)	Y	Y	Y	Y	N	N	N	Y	N	High bandwidth consumption
GBS-AKA [52,56]	Secure entity-based mutual authentication	Y	N	Y	N	Y	N	N	Y	Y	Weak unlink-ability (both KFS/KBS)
SEGB-AKA [39]	Public key-based mutual entity authentication	N	Y	Y	Y	N	N	Y	Y	Y	Weak unlink-ability (both KFS/KBS)

Note: Y: Yes. N: No, S1: Integrity, S2: Confidentiality, S3: Authentication, S4: Privacy Preservation, T1: MiTM, T2: DoS attacks, T3: Impersonation attack, T4: Node-Replication Threat, T5: Spoofing.

3.2 Local Authentication

Local authentication is adopted when devices are near or in close vicinity. It requires user equipment to be within reach of MTC devices and does not require Internet or remote access. For example, for patients' clinical tests via sensors, the patient has to be available within the medical facility. Similarly, for sensitive laboratories, the door has to be opened by the user through RFID

(radio frequency identification), thus accessing the facilities only, and smart parking where parking space is allocated to drivers within the parking station [23]. In such circumstances, local authentication is more suitable and less costly regarding security and operational feasibility. However, unlike the GBA schemes, the communication protocols are less robust than those of 4G or mobile networks. This is why operating local authentication-based systems is challenging [1], especially when numerous users are authenticated simultaneously. Local authentication is usually designed for access control systems where users have different privileges, such as two users with different hierarchies. One is granted full access, while the other is granted half access for certain system features. The local authentication network consists of M2M devices, a gateway, and communication channels where gateways can transfer data over the Internet and the cloud. During the transmission, the M2M device encounters three major challenges.

- All devices must be authenticated to ensure secure data transfer because an impersonator can easily use fake nodes to monitor data transmission and obtain crucial information related to security. In contrast, with malicious nodes, the integrity of the entire network could be at risk. To authenticate both, a mutual authentication scheme is mostly adopted [57]. Mutual authentication in MTC devices happens with encrypted shared keys. These keys are generated via symmetric or asymmetric crypto-mechanism with the cost of complex MAC and high computation power.
- All M2M communicating devices must ensure user privacy through anonymity. It is very crucial to ensure secrecy. During communication, MTC devices must not share any data relating to the data sender's identity [58]. If such privacy is neglected, logs generated by devices may reveal sensitive information related to who, when, and where access was granted to a particular privileged user. Furthermore, a service provider could also reveal the information of all M2M devices' access control operations. That is why anonymity will ensure that the information is kept hidden from other devices [26,59].
- Since MTC devices possess low computational power, limited memory, and heterogeneity with dynamic topology, computational complexity must be designed so that 8-16-bit microprocessors can process smoothly. These limitations make the authentication process more difficult as traditional robust authentication methods may strain the limited resources. Complex encryption algorithm implementation may result in higher processing demands, which could impair the device responsiveness and performance.

Thus, it becomes essential to strike a balance between the requirement to save resources and strong security measures in order to guarantee that the authentication process stays efficient without unnecessarily straining the limited capabilities of MTCDs. Lightweight cryptography is also adopted to ensure privacy and mutual authentication. However, achieving all basic security features with efficiency is an ongoing research.

Table 6 provides a summary of local authentication schemes according to Table 4. Local authentication and access scheme in WSN (wireless sensor network) using a public key with a symmetric cryptosystem for healthcare applications was proposed by Le et al. [60]. Sensor nodes' task was to perform symmetric-key encryption computation and were verified online by third-party coordinate nodes. Shen [61] designed a user access control scheme based on a symmetric encryption system using Merkle tree and hash chain functions. The scheme reduced space complexity but did not achieve basic security features. Due to compromised user anonymity, a user's sensitive information is exposed during communication. Wang et al. [62] introduced hybrid authentication by merging local and remote access control system features and incorporating ECC (elliptical curve cryptography) lightweight

cryptography [63]. However, the sensor authentication property is ignored and thus is vulnerable to impersonator/fake nodes. Zhang et al. [36] proposed RSA (Rivest-Shamir-Adleman)-based blind signatures as tokens for users to obtain access rights. The proposed mechanism ensured user privacy and sensor node anonymity. He et al. [35] highlighted that Zhang's mechanism did not account for double-spending, resulting in heavy memory consumption and network overheads. He et al. introduced an improved mechanism version by adding ring signatures based on elliptic curve cryptography to achieve user anonymity and reduce memory and communication overheads. The technique was also vulnerable to MiTM attacks using the ECDH (elliptic curve Deffie-Hellman) algorithm [63]. He et al. further attempted to improve the scheme by adding node accountability [64] to implement network-based rules. Sophisticated privacy-ensuring mechanisms resulted in high computation costs and memory consumption, which MTC devices cannot afford. Similar related works [60–62] aimed to compensate operations in resource-constrained MTC devices by ignoring privacy. Both schemes [60,62] are based on certificate-based authentication. Users can identify logs and logging activities by verifying their certificates. On the contrary, references [36,64] required the MTC devices to execute complex computation for acheivement of privacy. Furthermore, references [35,36], and [61,62] did not incorporate device authentication properly and lacked in achieving basic security features. Meanwhile, computational tasks are offloaded to another powerful sever to mitigate MTC devices' computational and memory overheads while achieving privacy and efficiency. However, it is challenging as the whole network relies on the server for computations. Any delay in servers can result in increased latency and network losses. In [60], mutual authentication is carried out through the authority of coordinated nodes despite authenticating each node directly. However, the user cannot access sensor nodes when controlled by coordinate nodes if coordinate nodes face any malfunction. Cai et al. [1] proposed a scheme that improve resource management for resource-constrained MTC devices inclduing user anonymity where computation is transferred to third part server which authenticates all devices via pre-shared keys. However, the mechanism could not perform well in noisy signals and did not register lost bytes in noisy signal losses. The proposed mechanism is also prone to failure if the authenticating server either loses the communincation ability or malfuncations. Moreover, there are security problems in the schemes where users' secrets are unprotected throughout the communication. He et al. [64] accomplished user privacy in contradiction to the service provider but their proposed method consumes more energy. Energy consumption increases with the increase of group member devices sharing similar access privileges. The schemes of [36] and [62] devour continuous energy for the MTC device for every user access operation despite unguaranteed user privacy. For the execution costs on MTC devices and users, proposed schemes [35,61,62] need to include a certificate generation and verification function, which necessitate exponentiation and inversion executions. Furthermore, associated with [35], LACS's multiplication cost does not raise with the increase in group members. However, references [61,62] cost significantly more energy.

Table 6: Summary of mentioned local authentication schemes

Schemes	Achievements	Basic security features				Threat vulnerabilities					Weaknesses
		S1	S2	S3	S4	T1	T2	T3	T4	T5	
[60]	Resource constraint authentication	N	Y	Y	N	Y	N	Y	Y	Y	User privacy is ignored
[61]	Reduced memory consumption	N	N	N	N	Y	N	Y	Y	Y	Sensor node authentication is ignored

(Continued)

Table 6 (continued)

Schemes	Achievements	Basic security features				Threat vulnerabilities					Weaknesses
		S1	S2	S3	S4	T1	T2	T3	T4	T5	
[62]	Distributed access control for local and remote access	N	N	Y	N	Y	N	Y	N	Y	Sensor node authentication is ignored
[35]	Group-based ring signatures	Y	N	Y	Y	Y	N	Y	Y	N	Sensor node authentication is ignored
[36]	Token-based authentication	Y	N	Y	Y	Y	Y	Y	Y	N	Double-spending tokens consume more memory
[64]	Improved security via network-based rules	Y	Y	Y	Y	N	Y	N	N	N	High computational and network overheads
[1]	Computational offloading	N	Y	Y	Y	Y	N	N	N	Y	Network vulnerable to failure if a server does malfunction

Note: Y: Achieved, N: Not Achieved, S1: Data integrity, S2: Mutual Authentication, S3: Key Confidentiality, S4: User Privacy, T1: MiTM, T2: DoS attacks, T3: Impersonation attack, T4: Node-Replication Threat, T5: Spoofing.

3.3 Factor-Based Authentication

Apart from group and local-based authentication, several other works have been proposed in securing MTC device communication with efficiency by adding additional unique parameters, including encryption, pre-shared unique identity keys, two factors such as user and device by using encrypted keys, three-factor such as user to device and device to the gateway, device signatures and implementing secure hash-functions. Each parameter is addressed to a particular environment and topological structure of the WSN network. Such authentication schemes are used for specific business applications requiring specific networks with user-controlled privileges.

Table 7 summarizes hybrid and factor-based authentication schemes analyzed through features presented in Table 4. Das [65] proposed a two-factor user verification method for WSN by securing secret key risking, mimicking, and DoS attacks. Vaidya et al. [66] pointed out that such a scheme had some security flaws by not offering users to change passwords and shared authorization between the gateway, sensors, and nodes. Vaidya et al. brought up a strategy that proposed an improved method. However, the proposed method offered no defense against malicious insider and brute-force attacks [67]. Additionally, they proposed a scheme to counter such attacks by merging keys and XORing the results. However, the scheme could not withstand insider and disconnected secret key-guessing attacks. Reference [11] devised a simple architecture for mutual authentication by prioritizing low computational and lesser memory consumption. The scheme met low computation and less memory consumption criteria but lacked database-related security measures. Reference [13] proposed an improved AKA scheme specifically for M2M correspondences in 6LoWPAN (IPv6 over low-power wireless personal area networks) systems. To overcome the weaknesses referenced in AKAES (authentication and key agreeing encrypted system), a combination of cryptography is utilized for secure authentication and shared keys with thought of resource constraints at 6LoWPAN utilizing MTC devices. A handover ticket is produced for a mobile device (6LR) to accomplish quick authentication when performing handovers. Therefore, a full authentication process may be performed once the ticket is terminated. In addition, the proposition has a remarkable element of giving security backing to both static and portable devices in 6LoWPAN systems. Reference [68] proposed model of authentication using IBC (Identity Based Cryptography) known as AIBCwKE (authentication via

identity-based cryptography without key escrow), where all devices were assigned encrypted identities via ECC cryptography, excluding key agreeing mechanisms by third parties. The MSP (Machine to Machine Service Provider) was the main connectivity server and established communication between two entities (device, gateway, and user) using a public key. Reference [69] proposed three-factor authentication to target user anonymity, an extension to [70] and [71]. Jiang et al. [70] incorporated two-factor-based ECC authentication where a user would log in, authenticate, and share data. Only the shared was encrypted by lightweight cryptography based on ECC, thus achieving data integrity and a low resource-occupying mechanism, an extension of [71]. Choi et al.'s work [71] proposed an enhanced scheme to improve its predecessor's ECC techniques for user anonymity. The proposed mechanism improved authentication and disabled security faults through BAN logic. Reference [69] discussed security flaws in [70] and pointed to a lack of user-friendliness, password updating method, and missing function to detect unauthorized login.

Table 7: Summary of discussed factor-based schemes in M2M communicating networks

Schemes	Factors	Achievements	Basic security features				Threat vulnerabilities					Weaknesses
			S1	S2	S3	S4	T1	T2	T3	T4	T5	
[65]	User verification and pre-shared keys	Oppose key guessing attacks	N	Y	N	Y	Y	N	Y	Y	Y	Password updates and shared authorization are ignored
[66]	Login and user authentication	Improved two-factor authentication	N	Y	Y	Y	Y	N	Y	Y	Y	Weak against Malicious insider and password-guessing attacks
[70]	ECC-based two-factor authentication	User and login-based authentication	Y	Y	N	Y	N	Y	N	Y	Y	User-friendliness and password-changing methods
[11]	Pre-shared keys	Low computational and less memory consumption	N	Y	Y	N	Y	Y	Y	Y	N	Physical layer M2M security is Ignored.
[13]	EASKES6LO	AKA for 6LOWPAN	Y	Y	N	Y	Y	N	N	N	N	Presumed smaller threat model for test
[68]	AIBCwKE	Hybrid key-based secure communication	Y	Y	Y	Y	Y	N	Y	N	N	Public key with MSP creates computational and network overheads
[71]	BAN logic	Mutual authentication	N	Y	Y	Y	Y	N	Y	Y	Y	Data not secured during transmission
[69]	User biometric signature	Novel password mechanism	Y	Y	Y	N	Y	N	N	N	N	Biometric signature is required for all nodes

Note: Y: Achieved, N: Not Achieved, S1: Data integrity, S2: Mutual Authentication, S3: Key Confidentiality, S4: User Privacy, T1: MiTM, T2: DoS attacks, T3: Impersonation attack, T4: Node-Replication Threat, T5: Spoofing.

4 Issues and Challenges

The evidence from Tables 5–7 suggests that the methods with good encryptions successfully achieved data integrity. Good encryption on data transmission ensured countering the MiTM attacks and data spoofing attacks. Meanwhile, the schemes with mutual authentication and good encrypted keys achieved user and device privacy. Schemes with only key encryption techniques are liable to MiTM and impersonator attacks because an impersonator can guess that the encrypted MACs are predominantly keys, so it will be easier to retrieve secrets. However, to our knowledge, an efficient scheme with end-to-end encryption, encrypted keys, and mutual authentication has not been found

in any of the mentioned authentication types. The two-layer encryption would prove robust against MiTM and spoofing attacks while ensuring user and device privacy, including authentication. On the contrary, efficient two-layer encryption for keys and end-to-end encryption would be challenging as it might produce network overheads and prove costly in computation and memory consumption. Achieving optimal security protocol for MTC devices is still challenging because many devices work simultaneously in one network.

Our study elaborates on the weaknesses and strengths of current protocols and schemes used to counter certain challenges in communication, as discussed in the following. Fig. 3 shows a taxonomy of authentication schemes used in M2M communication.

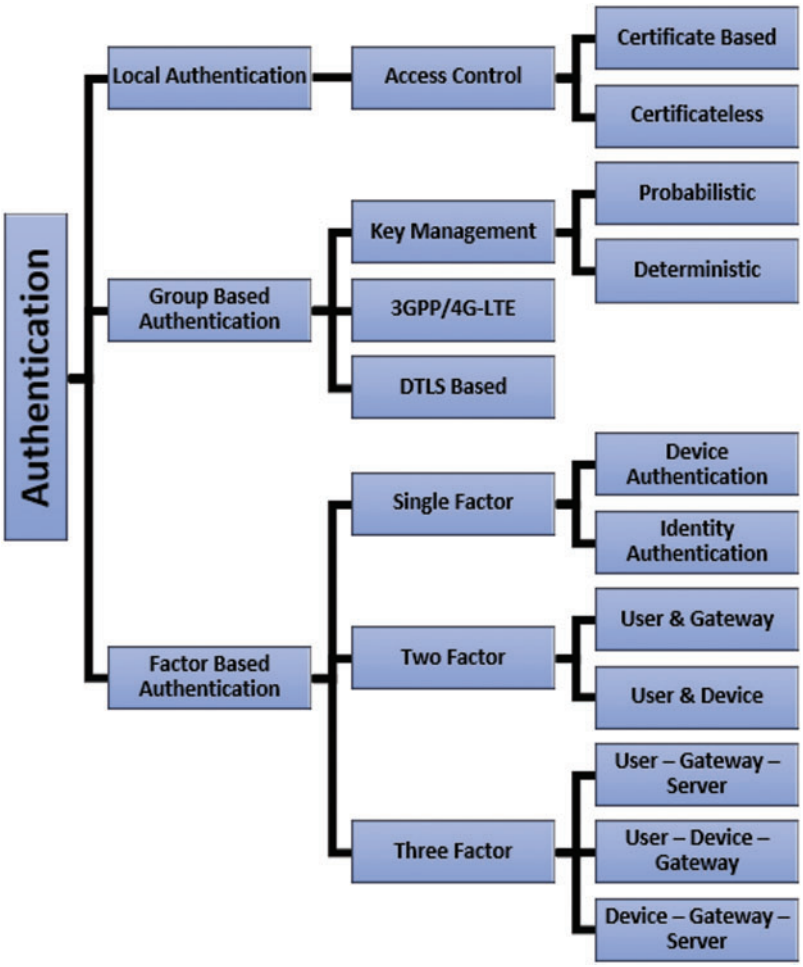

Figure 3: Taxonomy of authentication in M2M communication

- Groups-based authentication suits a network of large amounts of devices that require remote access via the Internet or use cloud services for data storage and access control. Such schemes require 3GPP or 4G infrastructure that provides seamless connectivity for remote users and mobility for mobile devices. However, MiTM and spoofing attacks are yet to be encountered efficiently in remote areas.

- Local authentication schemes better counter MiTM and Spoofing attacks due to easy access in sensitive and crucial business applications, which must ensure user privacy. That is why security features must be addressed, assuming risky threat models. However, efficient computational power and memory consumption are still lacking in the proposed schemes in Table 5.
- With no 3GPP or 4G infrastructure, several devices must communicate simultaneously via a well-organized network that ensures user privacy and mutual authentication. However, forward and back security is still challenging for such big networks. The risk extends to the whole network if a single device faces vulnerability. A complete collision detection text must be taken out for all devices in the network, which is time-consuming, costly, and highly complex.
- No scheme mentioned in this article addressed data availability during communication failure scenarios. If the network faces communication failure for any reason, the devices will also lose functionality and data. A system enabling such devices to work even during communication failure is still challenging.
- There is a gap in achieving a standard authentication model for a general authentication scheme that can address all general M2M communication applications.

5 Conclusion

In conclusion, establishing fool-proof security in the domain of Internet of Things (IoT) remains a formidable challenge. Authentication, as a fundamental component of security provisions, plays a crucial role in ensuring the integrity and confidentiality of Machine-Type Communication (MTC) devices. Our study delves into various authentication techniques aimed at achieving optimal performance efficiency and security while minimizing associated costs. The investigation sheds light on persistent challenges and outlines potential avenues for enhancing security in the future. Despite the advancements in two-layer encryption, which ensures user and device privacy and guards against spoofing and Man-in-the-Middle (MiTM) attacks, it comes with noticeable computational and network overheads. Group-based authentication emerges as a suitable solution for large networks, but its efficacy requires efficient countermeasures in remote areas. Local authentication schemes effectively address MiTM and spoofing attacks but encounter computational power challenges, while the unresolved issue of data availability during communication failures persists.

This study can further benefit from state-of-the-art techniques in the evolving landscape of IoT security, such as edge and fog computing, biometric authentication, blockchain-based authentication, risk-based authentication, machine learning, and anomaly detection. Furthermore, quantum-resistant authentication can be used to cope up with dynamic nature of IoT security. In this context, some prominent works on state-of-the-art concepts in IoT security can be used as a basis for further research, such as [72–74], that emphasizes who has described the security implications of quantum cryptography, artificial intelligence and lightweight peer-to-peer authentication. Additionaly, the research of Bonandrini et al. [75] has also contributed to anomaly detection in IoT networks, while researches in [76,77] proposed a Blockchain-based scheme for authentication and cloud based security in IoT environments. Furthermore, a secure authentication and protocol for M2M communication by Thammarat et al. [78] and the research of Zareen et al. [73] on authentication and authorization of IoT devices using AI can also be further research direction. These works further propose innovative approaches to address the multifaceted challenges in IoT security. As the field continues to evolve, embracing these trends and leveraging their unique contributions will be pivotal in establishing a standardized authentication model for general M2M communication applications.

Acknowledgement: The authors acknowledge the gracious support provided by the King Faisal University, Saudi Arabia.

Funding Statement: This work was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. GRANT5,208).

Author Contributions: The authors worked together on different parts of the research. S.U. started with problem formulation and conducted initial studies. S.U.B. performed problem analysis and critical review of related studies. M.I. checked for mistakes and planned research methodology. Q.M.I. and A.M. critically analyzed and interpreted the results. M.A.S. analyzed the research challenges, while M.A.R. and I.K. proposed potential future works. A.H. critically reviewed and revised the draft. S.I., Y.G., and K.H. helped with the manuscript write-up.

Availability of Data and Materials: All data used in this research are available from the corresponding authors upon request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Cai, P. Mao, Z. Wang, D. Wang, J. He and X. Fan, "Associations between problematic internet use and mental health outcomes of students: A meta-analytic review," *Adolesc. Res. Rev.*, vol. 8, no. 1, pp. 45–62, Mar. 2023. doi: 10.1007/s40894-022-00201-9.

[2] Statista, "Internet usage worldwide—statistics & facts," *Statista*. Accessed: Dec. 06, 2023. [Online]. Available: https://www.statista.com/topics/1145/internet-usage-worldwide/#topicOverview

[3] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective," *Sustainability*, vol. 15, no. 4, pp. 3317, Feb. 2023. doi: 10.3390/su15043317.

[4] N. G. Vasilescu, P. Pocatilu, and M. Doinea, "IoT security challenges for smart homes," in *Proc. 21st Int. Conf. Inf. in Eco. (IE 2022)*, Singapore, Springer Nature Singapore, 2023, pp. 41–49.

[5] Y. R. Shi and T. Hou, "Internet of things key technologies and architectures research in information processing," in *Proc. 2nd Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, France, Atlantis Press, 2013.

[6] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in *10th Int. Conf. Front. Inf. Technol. (FIT)*, Islamabad, Pakistan, IEEE, 2012, pp. 257–260.

[7] X. Yang, Z. Li, Z. Geng, and H. Zhang, "A multi-layer security model for internet of things," in *Internet of Things*, Springer, Changsha, China, 2012, pp. 388–393.

[8] Y. Zhang, "Technology framework of the Internet of Things and its application," in *2011 Int. Conf. Electric. Cont. Eng.*, Yichang, China, IEEE, 2011, pp. 4109–4112.

[9] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 296–312, Feb. 2023. doi: 10.1007/s11036-022-01937-3.

[10] V. G. Garagad, N. C. Iyer, and H. G. Wali, "Data integrity: A security threat for internet of things and cyber-physical systems," in *2020 Int. Conf. Comput. Performance Evaluation (ComPE)*, Meghalaya, India, IEEE, Jul. 2, 2020, pp. 244–249.

[11] B. D. Deebak and A. T. Fadi, "Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing," *Future Gener. Comput. Syst.*, vol. 116, no. 1, pp. 406–425, Mar. 2021. doi: 10.1016/j.future.2020.11.010.

[12] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wirel. Person. Commun.*, vol. 115, no. 2, pp. 1667–1693, Nov. 2020. doi: 10.1007/s11277-020-07649-9.
[13] P. M. Chanal and M. S. Kakkasageri, "Preserving data confidentiality in Internet of Things," *SN Comput. Sci.*, vol. 2, no. 1, pp. 53, Feb. 2021. doi: 10.1007/s42979-020-00429-z.
[14] M. Eckardt and W. Kerber, "Property rights theory, bundles of rights on IoT data, and the EU data act," *Eur. J. Law Econ.*, vol. 19, no. 5, pp. 1–31, Jan. 2024. doi: 10.1007/s10657-023-09791-8.
[15] D. Chen and G. Chang, "A survey on security issues of M2M communications in cyber-physical systems," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 1, 2012. doi: 10.3837/tiis.2012.01.002.
[16] V. L. Narayana and C. Bharathi, "Identity based cryptography for mobile ad hoc networks," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 5, p. 1173, 2017.
[17] D. Garcia-Carrillo, X. G. Pañeda, D. Melendi, R. Garcia, V. Corcoba and D. Martínez, "Ad-hoc collision avoidance system for industrial IoT," *J. Ind. Inf. Integration*, vol. 17, no. 1, pp. 100575, Jan. 2024. doi: 10.1016/j.jii.2024.100575.
[18] S. Bhasin and F. Regazzoni, "A survey on hardware trojan detection techniques," in *IEEE Int. Symp. Circ. Syst.*, Lisbon, Portugal, 2015, pp. 2021–2024.
[19] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, 2010. doi: 10.1109/MDT.2010.7.
[20] H. Tanaka, "Information leakage via electromagnetic emanation and effectiveness of averaging technique," in *2008. Int. Conf. Inf. Secur. Assur.*, Busan, Korea, IEEE, 2008, pp. 98–101.
[21] A. Brandt, J. Buron, and G. Porcu, "Home automation routing requirements in low-power and lossy networks," Internet Engineering Task Force (IETF), 2010.
[22] S. Seys and B. Preneel, "Authenticated and efficient key management for wireless ad hoc networks," in *Proc. 24th Symp. Inf. Theory Benelux*, Haasrode, Belgium, Werkgemeenschap voor Informatie-en Communicatietheorie, 2003, pp. 195–202.
[23] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 318–332, 2013. doi: 10.1109/TMC.2011.274.
[24] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ubiquitous computing," *Comput.*, vol. 35, no. 4, pp. supl22–supl26, 2002. doi: 10.1109/MC.2002.1012427.
[25] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur.*, Hong Kong, China, ACM, 2011, pp. 355–366.
[26] A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: A privacy-aware smart city is possible," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 136–141, 2013. doi: 10.1109/MCOM.2013.6525606.
[27] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: A smart spy in your home," *Black Hat USA*, 2014.
[28] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *2005 Symp. Secur. Priv.*, Oakland, CA, USA, 2005, pp. 49–63.
[29] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, 2007, vol. 1, pp. 367–409.
[30] D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv:0909.0576, 2009.
[31] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks," *Gen.*, vol. 15693, pp. 14443, 2010.
[32] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Comput. Sci. Rev.*, vol. 38, no. 7, pp. 100312, 2020. doi: 10.1016/j.cosrev.2020.100312.
[33] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," *Wirel. Netw.*, vol. 27, no. 8, pp. 5503–5509, 2021.
[34] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, 2020. doi: 10.1109/JIOT.2020.2969326.

[35] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 10, no. 10, pp. 3472–3481, 2011. doi: 10.1109/TWC.2011.072511.102283.

[36] R. Zhang, Y. Zhang, and K. Ren, "DP^{2}AC: Distributed privacy-preserving access control in sensor networks," in *IEEE INFOCOM 2009*, Rio de Janeiro, Brazil, IEEE, 2009, pp. 1251–1259.

[37] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet Things*, vol. 5, no. 3, pp. 1606–1615, 2017. doi: 10.1109/JIOT.2017.2787800.

[38] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 408–417, 2016. doi: 10.1109/JIOT.2015.2495321.

[39] B. L. Parne, S. Gupta, and N. S. Chaudhari, "SEGB: Security enhanced group based AKA protocol for M2M communication in an IoT enabled LTE/LTE-A network," *IEEE Access*, vol. 6, pp. 3668–3684, 2018. doi: 10.1109/ACCESS.2017.2788919.

[40] S. G. Oliver and T. Purusothaman, "Lightweight and secure mutual authentication scheme for IoT devices using CoAP protocol," *Comput. Syst. Sci. Eng.*, vol. 41, no. 2, pp. 767–780, 2022.

[41] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans. Ind. Inf.*, vol. 16, no. 11, pp. 7081–7093, 2019. doi: 10.1109/TII.2019.2942389.

[42] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Gener. Comput. Syst.*, vol. 78, no. 11, pp. 1005–1019, 2018. doi: 10.1016/j.future.2016.12.028.

[43] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security," *J. Amb. Intell. Human. Comput.*, vol. 8, no. 1, pp. 101–116, 2017. doi: 10.1007/s12652-016-0345-8.

[44] B. Blanchet, V. Cheval, X. Allamigeon, and B. Smyth, "ProVerif: Cryptographic protocol verifier in the computational model," Oxford, UK: IEEE, pp. 16–30, 2010.

[45] H. A. H. Hassan, A. Pelov, and L. Nuaymi, "Integrating cellular networks, smart grid, and renewable energy: Analysis, architecture, and challenges," *IEEE Access*, vol. 3, pp. 2755–2770, 2015. doi: 10.1109/ACCESS.2015.2507781.

[46] J. Mišić, V. B. Mišić, and N. Khan, "Sharing it my way: Efficient M2M access in LTE/LTE-A networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 696–709, 2017.

[47] K. R. Jung, A. Park, and S. Lee, "Machine-type-communication (MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network," in *Int. Conf. Securi-Enriched Urban Comput. Smart Grid*, Daejeon, Korea, Springer, 2010, pp. 167–178.

[48] Y. W. Chen, J. T. Wang, K. H. Chi, and C. C. Tseng, "Group-based authentication and key agreement," *Wirel. Person. Commun.*, vol. 62, no. 4, pp. 965–979, 2012. doi: 10.1007/s11277-010-0104-7.

[49] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, 2013. doi: 10.1016/j.comnet.2013.08.003.

[50] R. Jiang, C. Lai, J. Luo, X. Wang, and H. Wang, "EAP-based group authentication and key agreement protocol for machine-type communications," *Int. J. Distrib. Sens. Netw.*, vol. 9, no. 11, pp. 304601, 2013. doi: 10.1155/2013/304601.

[51] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 3, pp. 414–431, 2015. doi: 10.1002/ett.2635.

[52] D. Choi, H. K. Choi, and S. Y. Lee, "A group-based security protocol for machine-type communications in LTE-advanced," *Wirel. Netw.*, vol. 21, no. 2, pp. 405–419, 2015. doi: 10.1007/s11276-014-0788-9.

[53] J. Cao, M. Ma, and H. Li, "GBAAM: Group-based access authentication for MTC in LTE networks," *Secur. Commun. Netw.*, vol. 8, no. 17, pp. 3282–3299, 2015. doi: 10.1002/sec.1252.

[54] A. Fu, J. Song, S. Li, G. Zhang, and Y. Zhang, "A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2002–2014, 2016. doi: 10.1002/sec.1455.

[55] C. Lai, R. Lu, D. Zheng, H. Li, and X. S. Shen, "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications," *Comput. Netw.*, vol. 99, no. 4, pp. 66–81, 2016. doi: 10.1016/j.comnet.2016.02.007.

[56] J. Yao, T. Wang, M. Chen, L. Wang, and G. Chen, "GBS-AKA: Group-based secure authentication and key agreement for M2M in 4G network," in *Int. Conf. Cloud Comput. Res. Innov. (ICCCRI)*, Singapore, IEEE, 2016, pp. 42–48.

[57] Krebsonsecurity, "all about skimmers," 2017. Accessed: Dec. 06, 2023. [Online]. Available: http://krebsonsecurtiy.com/all-about-skimmers/

[58] K. Islam, W. Shen, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," in *Proc. 2012 IEEE 16th Int. Conf. Comput. Support. Cooperat. Work Des. (CSCWD)*, Wuhan, China, IEEE, 2012, pp. 626–633.

[59] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 981–997, 2012. doi: 10.1109/SURV.2011.122111.00145.

[60] X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *J. Netw.*, vol. 6, no. 3, pp. 355, 2011. doi: 10.4304/jnw.6.3.355-364.

[61] Y. Shen, "An access control scheme in wireless sensor networks," in *Proc. 4th IFIP Int. Conf. Netw. Parallel Comput. Works. (NPC2007)*, USA, Sep. 2007, pp. 362–367.

[62] H. Wang and Q. Li, "Achieving distributed user access control in sensor networks," *Ad Hoc Netw.*, vol. 10, no. 3, pp. 272–283, 2012. doi: 10.1016/j.adhoc.2011.01.011.

[63] D. Hankerson, A. J. Menezes, and S. Vanstone, "Guide to elliptic curve cryptography," *Comput. Rev.*, vol. 46, no. 1, pp. 13, 2005.

[64] D. He, S. Chan, and M. Guizani, "Accountable and privacy-enhanced access control in wireless sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 1, pp. 389–398, 2015. doi: 10.1109/TWC.2014.2347311.

[65] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 3, pp. 1086–1090, 2009. doi: 10.1109/TWC.2008.080128.

[66] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *Wirel. Mobile Comput., Netw. Commun. (WiMob), 2010 IEEE 6th Int. Conf.*, Niagara Falls, Canada, IEEE, 2010, pp. 600–606.

[67] W. B. Hsieh and J. S. Leu, "A robust ser authentication scheme sing dynamic identity in wireless sensor networks," *Wireless Person. Commun.*, vol. 77, no. 2, pp. 979–989, 2014.

[68] S. Chen, M. Ma, and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 1146–1157, 2016. doi: 10.1002/sec.1407.

[69] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, 2018. doi: 10.1016/j.jnca.2017.07.001.

[70] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, no. 1, pp. 37–48, 2016. doi: 10.1016/j.jnca.2016.10.001.

[71] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sens.*, vol. 14, no. 6, pp. 10081–10106, Jun. 2014. doi: 10.3390/s140610081.

[72] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Netw. Secur.*, vol. 2020, no. 9, pp. 9–15, 2020. doi: 10.1016/s1353-4858(20)30105-7.

[73] M. S. Zareen, S. Tahir, and B. Aslam, "Authentication and authorization of IoT edge devices using artificial intelligence," in D. Cham, D. Puthal, S. Mohanty, B. Y. Choi (Eds.), *Internet of Things. Advances in Information and Communication Technology*. Switzerland: Springer Nature, 2024, pp. 442–453.

[74] Y. Zheng, W. Liu, C. Gu, and C. H. Chang, "PUF-based mutual authentication and key exchange protocol for peer-to-peer IoT applications," *IEEE Trans. Depend. Secure Comput.*, 2022.

[75] V. Bonandrini, J. F. Bercher, and N. Zangar, "Machine learning methods for anomaly detection in IoT networks, with illustrations," in *Machine Learning for Networking*, Paris, France, 2019, pp. 287–295.

[76] N. Sivaselvan, K. B. Vivekananda, and M. Rajarajan, "Blockchain-based scheme for authentication and capability-based access control in IoT environment," in *2020 11th IEEE Annual Ubiquit. Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 28–31, 2020, pp. 0323–0330. doi: 10.1109/UEMCON51285.2020.9298116.

[77] P. K. Panda and S. Chattopadhyay, "An enhanced mutual authentication and security protocol for IoT and cloud server," *Inf. Secur. J.: A Global Perspect.*, vol. 31, no. 2, pp. 144–156, 2022. doi: 10.1080/19393555.2020.1871534.

[78] C. Thammarat and C. Techapanupreeda, *A Secure Authentication and Key Exchange Protocol for M2M Communication*. 2021. [Online]. Available: https://dx.doi.org/10.1109/iEECON51072.2021.9440355