International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 4, August 2025, pp. 4249~4258
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i4.pp4249-4258

Privacy and confidentiality in internet of things: a literature review

Hiba Kandil, Hafssa Benaboud
Intelligent Processing and Security of Systems, Faculty of Sciences, Mohammed V University in Rabat, Rabat, Morocco

Article Info

Article history:

Received Sep 7, 2024
Revised Apr 14, 2025
Accepted May 24, 2025

Keywords:

Authentication
Authentication and trust in internet of things
Confidentiality
Internet of things
Privacy
Trust

ABSTRACT

The internet of things (IoT) is a scalable network of interconnected smart devices that aims to improve quality of life, business growth, and efficiency across multiple sectors. Since the IoT is an expanding network, a large amount of data is generated, collected, and exchanged. However, most of this data is personal data that contains private or sensitive information, which makes it a target for several cyber threats due to poor encryption, weak authentication mechanisms, and insecure communications. Therefore, ensuring the privacy and confidentiality of sensitive information remains a critical challenge. This paper presents a comprehensive literature review focusing on privacy and confidentiality issues within the IoT ecosystem. It categorizes existing research into privacy-preserving techniques, authentication and trust mechanisms, and machine learning-based solutions. Beginning by detailing the review methodology employed to gather and analyze relevant research. The review then explores recent research work related to privacy concerns and authentication and trust mechanisms, emphasizing various approaches and solutions developed to address these challenges. The paper further delves into machine learning-based solutions that offer innovative methods for enhancing privacy and confidentiality.

Corresponding Author:

Hiba Kandil
Intelligent Processing and Security of Systems, Faculty of Sciences, Mohammed V University in Rabat
Avenue Ibn Battouta B.P. 1014 RP, Rabat, Morocco
Email: hiba_kandil@um5.ac.ma

1. INTRODUCTION

The internet of things (IoT) is a fast-increasing network of connected things or objects that are embedded with intelligence and operate without human intervention. These smart things help IoT systems to provide advanced services in various areas that promise human life, such as healthcare, public surveillance, advanced building management systems, smart cities, decision-making, and more. Therefore, the IoT network generates, collects, and exchanges vast amounts of personal data such as user preferences, behavioral patterns, and sensitive health-related information. This sensitive data exchanged between IoT system components is typically unprotected due to the nature of IoT systems, which facilitate anytime, anywhere interactions with heterogeneous objects. Ensuring the security of a system is fundamental to the good functioning and adoption of any system. Security involves protecting all components of a system, which are data, software, and hardware, to protect critical systems from unauthorized access, theft, alteration, and various risks. Therefore, the security requirements of an IoT system are crucial to ensure the privacy, integrity, confidentiality, trust, and availability of the heterogeneous interconnected objects.

The diverse nature of IoT applications presents unique privacy and confidentiality challenges, especially as the use of IoT expands over vital sectors as healthcare, industry, and smart homes. In healthcare, for example, wearable devices and medical sensors collect sensitive health data that must be protected to ensure patient privacy and comply with regulatory requirements. Similarly, in smart homes and cities, IoT-enabled devices gather information about individuals' behaviors, preferences, and movements, raising concerns about surveillance and data misuse. We summarize in Table 1 some IoT applications with their impact on privacy and confidentiality.

Table 1. IoT applications and their impacts on privacy and confidentiality

IoT applications and/or devices	Benefits	Impact on privacy and confidentiality
Smart home devices	IoT devices in smart homes, such as smart thermostats, security cameras, and voice assistants, can collect vast amounts of data about residents' activities, preferences, and routines, and offer convenience and automation	IoT devices in smart homes raise concerns about unauthorized access to personal information and potential breaches of privacy.
Wearable health devices	Wearable health devices, such as fitness trackers and smartwatches, monitor users' biometric data, exercise routines, and sleep patterns. Providing valuable insights into users' health and fitness.	Wearable health devices raise privacy concerns regarding the collection, storage, and sharing of sensitive health information. Unauthorized access to this data could lead to privacy breaches and identity theft.
Smart city infrastructure	Smart sensors, traffic cameras, and public transportation systems collect data on traffic patterns, air quality, and energy consumption. These technologies improve urban infrastructure and services, and offer benefits such as improved traffic management and environmental monitoring.	IoT technologies in smart cities raise privacy concerns related to surveillance, tracking, and data sharing among government agencies and private companies.
Industrial IoT (IIoT)	IoT devices are used to monitor and control machinery, optimize production processes, and collect data for predictive maintenance. IIoT technologies offer benefits such as increased efficiency and productivity.	Unauthorized access to industrial IoT systems could result in sabotage, intellectual property theft, or disruptions to critical infrastructure.
Healthcare IoT	IoT devices such as medical sensors, remote monitoring devices, and connected medical equipment collect and transmit patient data for diagnosis, treatment, and remote patient monitoring. These technologies offer benefits such as improved patient care and reduced healthcare costs.	Unauthorized access to healthcare IoT systems could compromise patient confidentiality, lead to medical identity theft, or result in the unauthorized disclosure of personal health information.
Smart retail	IoT technologies are used in retail environments to track inventory, monitor customer behavior, and personalize shopping experiences. Smart shelves, radio frequency identification (RFID) tags, and beacons collect data on product movement and customer preferences to optimize store layouts and promotions. These technologies offer benefits such as improved inventory management and targeted advertising.	Unauthorized access to retail IoT systems could result in the collection and misuse of sensitive customer information.
Agricultural IoT	IoT devices such as soil sensors, weather stations, and drones are used to monitor crop conditions, optimize irrigation, and increase crop yields. IoT technologies enable precision agriculture practices that can reduce water usage, minimize pesticide use, and improve crop productivity.	Unauthorized access to agricultural IoT systems could compromise farmers' proprietary data, intellectual property, and trade secrets.
Connected cars	Connected car systems collect data on vehicle performance, driver behavior, and location for purposes such as maintenance scheduling, navigation, and insurance pricing. Being integrated into automobiles, IoT technologies enable features such as remote diagnostics, vehicle tracking, and autonomous driving. Improving safety and convenience.	Unauthorized access to connected car systems could compromise driver privacy, lead to vehicle theft, or result in safety hazards.
Environmental Monitoring	Sensors collect data on pollution levels, water contamination, and wildlife behavior to support environmental conservation efforts and public health initiatives. These technologies offer benefits such as early detection of environmental hazards and protection of natural resources.	Unauthorized access to environmental IoT systems could result in the manipulation of sensor data or the disruption of environmental monitoring efforts.
Energy management	Smart meters, energy monitors, and demand-response systems collect data on energy consumption patterns, identify energy inefficiencies, and optimize energy usage. These technologies offer benefits such as reduced energy costs and improved grid reliability.	Unauthorized access to energy IoT systems could result in the manipulation of energy usage data or the disruption of critical infrastructure.

Many reviews and surveys have been conducted in the literature to address privacy and confidentiality in the IoT environment. The paper [1] offers a detailed survey on implementing differential privacy in critical infrastructure enabled by IoT in smart grids, intelligent transport systems, healthcare and industrial IoT, covering the main application domains in detail. A summary of research efforts to address security and privacy issues using machine learning algorithms in the IoT from 2008 to 2019 is provided in [2] and [3]. Another survey is given in [4] in 2023. The paper provides an extensive survey of machine learning and deep learning solutions for IoT privacy, analyzing existing threats and attacks. It offers detailed examinations of various machine learning (ML) architectures, including implementations and outcomes. A comprehensive overview of AI-Driven behavioral analysis for security in IoT is given in [5]. The papers [6]–[14] provide reviews and surveys in the same fields. These articles provide an overview, comparison, and analysis of existing authentication mechanisms and protocols in IoT systems. They cover various aspects such as security issues, requirements, authentication schemes, protocols, and their benefits and drawbacks. The works also categorize authentication protocols based on different criteria and provide information on threat models, countermeasures, and formal security verification techniques used in IoT authentication. Although these works provide important surveys in the field of privacy and security in the Internet of Things, neither has presented a deep analysis of the recent existing contributions in privacy and confidentiality and ML-based solutions to address these challenges.

In this review, we provide an in-depth examination of the impact of privacy and confidentiality on IoT applications, explore various recent research efforts in privacy and confidentiality and ML-based solutions for privacy and confidentiality to outline the main IoT applications and the security requirements considered for each contribution, and we identify emerging research gaps and propose recommendations for building more resilient IoT systems. This paper is organized as follows. Section 2 provides the methodology followed for the literature review. Section 3 gives the literature review. It is categorized into three parts. The first part discusses related work on privacy in IoT, the second part covers papers related to confidentiality in IoT, and the final part cites related papers on machine learning-based solutions for both privacy and confidentiality in IoT. A summary of the research discussed, outlining the main IoT applications and the security requirements covered for each contribution in section 4. Section 5 concludes the paper.

2. REVIEW METHODOLOGY

Several studies have been conducted to address privacy and confidentiality in IoT. This section presents the proposed review methodology. For privacy in IoT, some of the recent existing efforts are provided in section 3.1. Besides, the study is divided into five categories based on the topics covered, including:

a. Privacy-enhancing techniques in healthcare IoT [15], [16]: These works focus on enhancing privacy protection in IoT-based healthcare applications using techniques such as homomorphic encryption, blockchain technology, and hierarchical blockchain models.
b. Differential privacy in IoT [17]: Differential privacy is a concept in data privacy that aims to protect sensitive information by adding random noise to query results or data itself. These works introduce differential privacy-based approaches and architectures to enhance privacy in IoT environments.
c. IoT data privacy frameworks [18]: These works present a generic framework for IoT data and location privacy. They analyze potential privacy threats and propose solutions to protect IoT users' privacy.
d. Privacy-preserving techniques for IoT data analytics [19]–[22]: These works introduce various privacy-preserving techniques for IoT data analytics, including privacy-preserving face representation schemes, raw data collection systems, source location privacy protection systems, and sophisticated interaction models.
e. Privacy-preserving solutions in IoT smart city applications [23]–[25]: These works propose privacy-preserving solutions for IoT-based smart city applications. They leverage technologies such as software defined networking (SDN), identity-based encryption schemes, and authentication protocols to ensure privacy, accountability, and security in data transmission and device authentication.

For the confidentiality in IoT, some of the recent existing efforts in the domain of authentication and trust in IoT are presented in section 3.2. The efforts are divided into three categories based on the topics covered, including:

a. Blockchain-based authentication in IoT [26]–[29]: These papers propose authentication mechanisms and trust management solutions based on blockchain technology for securing heterogeneous IoT systems and smart cities. They leverage lightweight cryptographic schemes, message integrity techniques, and facial recognition machine learning schemes to enhance authentication efficiency, data integrity, non-repudiation, and continuous authentication in IoT environments.
b. Trust management and biometric-based authentication in IoT [30], [31]: These papers propose trust management techniques and lightweight multi-biometric authentication systems to improve accuracy, reduce latency, energy consumption, and enhance security in IoT environments. They alternate between uni-biometric and multi-biometric techniques based on trust levels, compute trust values using lightweight computations, and ensure protection against various attacks targeting IoT devices.
c. Encryption and secure communication protocols in IoT [32], [33]: This category focuses on encryption and secure communication protocols in IoT, addressing the need for robust mechanisms to safeguard data privacy and integrity.

Another interesting topic is discussed in this paper including ML based solutions to address privacy and confidentiality in IoT environment. This topic is categorized into three categories as follows:

a. Privacy-preserving data processing [34]–[37]: This category includes works that focus on leveraging machine learning algorithms to process IoT data while preserving the privacy of sensitive information. These solutions often employ techniques such as differential privacy, federated learning, homomorphic encryption, convolutional neural networks, and generative AI to ensure confidentiality.
b. Anomaly detection and threat identification [38]–[41]: In this category, the emphasis is on using machine learning models to detect anomalies and identify potential threats to privacy within IoT networks. These solutions employ techniques like anomaly detection algorithms, supervised and unsupervised learning methods, generative adversarial networks, transfer learning, and deep learning approaches to identify abnormal behavior and unauthorized access attempts.
c. Secure data sharing and access control [42]: Works in this category aim to enable secure data sharing and enforce access control policies in IoT environments using machine learning techniques.

Figure 1 illustrates the various studies examined in this paper and their respective categories.

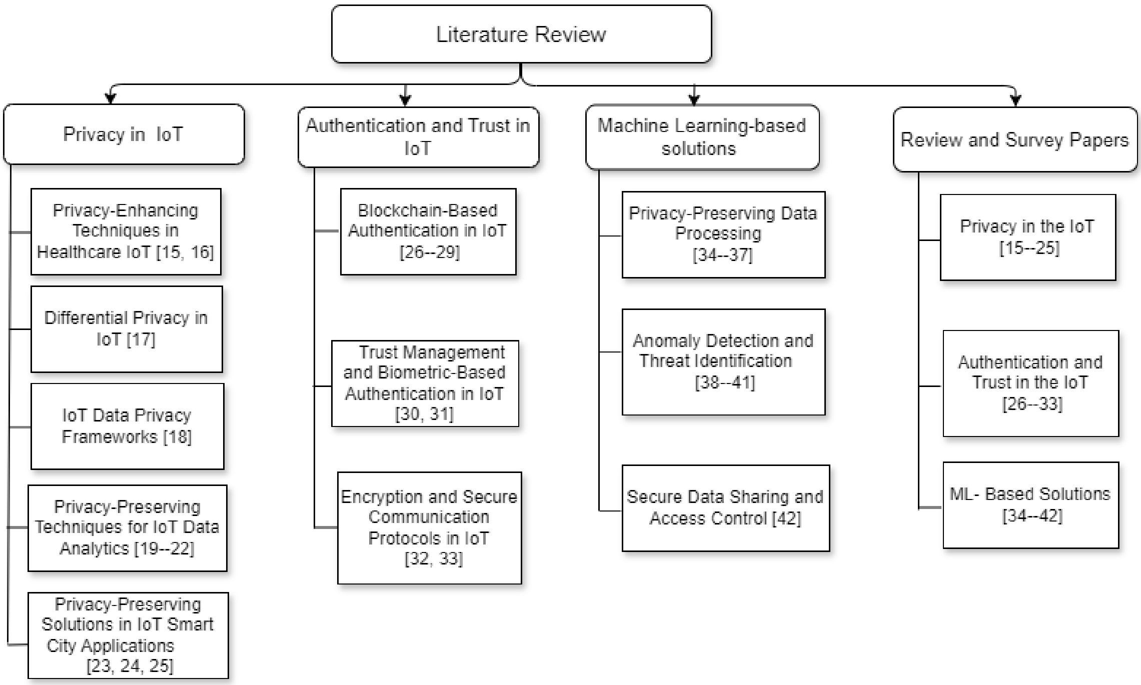
Literature Review
Privacy in IoT
Authentication and Trust in IoT
Machine Learning-based solutions
Review and Survey Papers
Privacy-Enhancing Techniques in Healthcare IoT [15, 16]
Differential Privacy in IoT [17]
IoT Data Privacy Frameworks [18]
Privacy-Preserving Techniques for IoT Data Analytics [19--22]
Privacy-Preserving Solutions in IoT Smart City Applications [23, 24, 25]
Blockchain-Based Authentication in IoT [26--29]
Trust Management and Biometric-Based Authentication in IoT [30, 31]
Encryption and Secure Communication Protocols in IoT [32, 33]
Privacy-Preserving Data Processing [34--37]
Anomaly Detection and Threat Identification [38--41]
Secure Data Sharing and Access Control [42]
Privacy in the IoT [15--25]
Authentication and Trust in the IoT [26--33]
ML- Based Solutions [34--42]

Figure 1. Reviewed papers on privacy and confidentiality in IoT

3. REVIEW STUDY

3.1. Related work to privacy in the IoT

In this part, some of the recent existing efforts for ensuring privacy in IoT are provided. The authors of [15] introduce an innovative and robust approach to bolster privacy safeguards in IoT-driven healthcare applications. They leverage homomorphic encryption techniques in conjunction with blockchain technology to fortify privacy measures. Their proposed model integrates smart contracts within the blockchain network to regulate access control and delineate data-sharing policies. Additionally, the model establishes an audit trail for all data transactions, thereby enhancing both accountability and transparency. Experimental findings underscore the efficacy of the solution in safeguarding data confidentiality while facilitating efficient data processing and analysis.

Esfahani *et al.* [16] present an alternative approach in healthcare IoT systems, introducing a three-layer hierarchical blockchain model designed to bolster data and location privacy against both internal and external threats. Furthermore, the proposed scheme offers features such as anonymous authentication, authorization, and scalability. Security analyses conducted demonstrated the robustness of the proposed model against a variety of attacks. In this category, Ali *et al.* [17] propose a novel three-way decisions-based strategy for achieving differential privacy, accompanied by an algorithm to effectively group attributes.

Additionally, they introduce a privacy-preservation architecture grounded in the principles of differential privacy. Experimental findings highlight the viability of this approach as a complementary method to augment the overall efficacy of differential privacy within IoT contexts.

Abuladel and Bamasag [18] have tackled the issue of unprotected data exchange among components within IoT systems. Additionally, they outline two use-case scenarios involving IoT users in healthcare applications, highlighting concerns regarding data and location privacy. Subsequently, the authors propose a comprehensive framework for safeguarding IoT data and location privacy and proceed to analyze potential privacy threats within this framework. Xue *et al.* [19] introduce an innovative privacy-preserving face representation scheme within the Bloom filter space. Unlike many existing schemes that focus on privacy-preserving analytic models derived from stored face data, this approach addresses privacy concerns at the end-device level. By doing so, it caters to the resource constraints of IoT devices, enabling analytics tasks to operate on privacy-preserving face data representations while preserving high data utility for analytics purposes.

In a different approach detailed in [20], a privacy-preserving raw data collection system for IoT is introduced. This system anonymizes participant data by merging it with data from other participants within a group, ensuring individual privacy is safeguarded. Notably, the original format of individual data is retained, enhancing its usability for data consumers. Moreover, this scheme operates without requiring a trusted central authority, making it suitable for real-world scenarios. Additionally, efficiency evaluations conducted through simulations demonstrate the practicality of this approach for IoT systems. Wang *et al.* [21] propose a source location privacy protection system known as ring-loop routing (SLPRR) for the IoT. To increase the adversary's backtracking time, the authors introduce a confounding time-domain transmission method to send real packets to a base ring. Additionally, phantom nodes, fake packets, and a confounding ring are utilized to protect the privacy of the source location. Analysis and experimental results have indicated that the proposed system can enhance security without impacting the network lifetime.

Another noteworthy privacy-preserving initiative is discussed in [22], where the authors introduce an intricate interaction model structured as a three-party game. This model tackles the issue of private data trading in IoT by taking into account the social connections and interactions of users within online social networks. Furthermore, considering the data trading between the service provider and the adversary as a Nash bargaining game, the authors have examined the Nash bargaining solutions through both theoretical analysis and numerical experiments. The analysis has effectively delineated the data trading strategies between the service provider and the adversary, offering valuable insights for the design of privacy protection schemes in IoT.

To address security and privacy challenges, Boussada *et al.* [23] have proposed an innovative privacy-preserving internet of things-based e-health solution that meets content and context privacy requirements. This solution accommodates the resource-constrained nature of IoT devices by leveraging a well-defined communication scenario and a novel identity-based encryption scheme. Furthermore, the authors have conducted a comprehensive security analysis to validate their proposal. In response to the limitations of existing privacy-preserving solutions, Gheisari *et al.* [24] have introduced the software defined networking (SDN) paradigm to IoT-based smart cities. They have developed an efficient privacy-preserving method to manage the flow of data packets from shared IoT device data. Additionally, extensive simulations using Mininet-WiFi have been conducted to showcase the effectiveness of their approach. Evaluation results demonstrate that compared to existing privacy-preserving solutions, the proposed method exhibits superior performance in terms of penetration rate, accuracy, and overhead for smart city applications.

In the same context, Wang *et al.* [25] have devised a privacy-preserving and accountable authentication protocol for IoT devices with weaker identities. This protocol integrates an adapted construction of short group signatures and a secret-sharing scheme. Furthermore, the authors have examined the security properties of the proposed protocol against six typical attacks and verified its formal security. Experimental results indicate that the authentication protocol is feasible in practice.

3.2. Related work on authentication and trust in the IoT

This part discusses some papers that treat authentication and trust in IoT. In study [26], a hybrid authentication architecture blending centralized and decentralized elements, leveraging blockchain and edge computing technologies, is presented for heterogeneous IoT systems. The implementation incorporates lightweight cryptographic schemes to enhance authentication efficiency and response time. Experimental results and security analyses underscore the model's resilience against attacks, demonstrating its capability to fulfill the security needs of IoT systems.

In [27], an alternative IoT authentication mechanism based on blockchain is introduced. The authors suggest an authentication and message integrity approach to facilitate cross-communication. Analysis results indicate its cost-effectiveness, efficiency, and suitability for distributed environments requiring cross-communication capabilities. In [28], another study on blockchain-based authentication is outlined, where the authors devise a secure and dependable authentication and trust management system tailored for smart cities using blockchain technology. Furthermore, they showcase a tangible application of this mechanism to safeguard the authorization of smart city assets. Additionally, they devise a hybrid application aimed at delivering a user-friendly interface for managing and interacting with the diverse objects within smart city environments.

The paper [29] introduces an innovative authentication solution leveraging blockchain technology. This approach provides a distributed and scalable authentication method. It facilitates real-time and non-intrusive continuous authentication in the IoT environment by initiating mutual initial static authentication between end-users and fog nodes to establish a secure encrypted channel. Additionally, the solution incorporates a trust module that utilizes facial recognition machine learning to identify outliers and anomalous access. Experimental findings highlight a lightweight, continuous authentication solution that effectively balances security objectives and performance requirements, thus addressing various common attacks targeting the IoT environment.

Modu *et al.* [30] introduce a lightweight multi-biometric system founded on trust management principles. This system aims to enhance accuracy while minimizing latency and energy consumption in IoT environments. It achieves this by employing a uni-biometric technique for trusted users and a multi-biometric approach for untrustworthy users. The energy efficiency and accuracy of the system are evaluated through hardware prototyping and discrete event simulation. Furthermore, the study analyzes the influence of trust management factors on performance metrics. Apte *et al.* [31] introduces a trust management technique centered around gateways and a procedure for calculating trust in IoT devices. The system prioritizes lightweight computations within devices, establishing trust between two objects through the computation of direct and indirect trust values. The findings demonstrate that the proposed system enhances the protection of IoT devices against diverse attacks.

In another approach aimed at safeguarding data confidentiality and fortifying internet of things devices against a range of attacks, Study by Sbaytri *et al.* [32] introduces a novel lightweight symmetric algorithm for encrypting/decrypting resource-constrained devices. This method employs irreversible elementary cellular automata to generate sub-keys and two-dimensional reversible cellular automata to facilitate substitutions and permutations. Analysis of the implementation indicates that the proposed cryptosystem exhibits a significant high avalanche effect, thereby enhancing the overall security level. Another paper for the category aimed on encryption of IoT protocols is [33]. The paper introduces a lightweight key synchronization update algorithm for a secure communication protocol, demonstrating resilience against common attacks like replay and man-in-the-middle attacks. Formal verification using Tamarin and performance evaluation show its superiority over other schemes in terms of randomness, computational performance, and utility.

3.3. ML-based solutions for privacy and confidentiality in IoT

Zhu *et al.* [34] propose a privacy-preserving ML training framework named Heda. The Heda framework offers privacy-preserving ML training using partial homomorphic encryption, ensuring security in aggregation scenarios and under collusion. Security analysis confirms protection in honest-but-curious models and against collusion, with experiments verifying its efficiency while maintaining model accuracy. Nonetheless, the solution necessitates computational efficiency and accuracy optimization for privacy-preserving ML training. In the same context, the paper [35] introduces a deep learning system for preserving privacy and analyzing IoT healthcare data, isolating privacy information at the user-end and conducting data analysis at the cloud-end. A security module based on convolutional neural networks is deployed, with extensive experiments demonstrating effectiveness and robustness. Although, the challenges caused by potential data breaches are admitted. Besides, deep learning model deployment in IoT healthcare demands sophisticated infrastructure.

Another work about real-time data processing and communication security in IoT suggests in [36]. This article investigates the combination of quantum computing, federated learning, and 6G wireless networks for securing future IoT systems. Besides, the authors discuss and analyze recent enhancements and issues in securing IoT systems. Furthermore, the paper introduces a novel approach integrating quantum technologies, federated learning within 6G networks to alleviate privacy and security in IoT. Meanwhile, the practical deployment of the proposed approach encounters difficulties due to technical and regulatory constraints. Quantum computing requires further research for integration in IoT security.

In [37], an investigation about data leaks and confidentiality issues in generative AI models. In addition, the paper introduces a secure and private system for generative AI with distributed computation on multiple nodes, dependence reduction on a single point of failure, and prevention of private data exposure to third-party AI providers. The approach secures user data and preserves the privacy of the AI models.

However, the scalable number of splits increases the network latency. The method requires optimizations in data load/offload among devices, and communication protocols efficiency.

For real-time anomaly detection, Shakya *et al.* [38] present a novel approach for IoT security that combines zero-trust security and AI/ML-driven threat detection, providing scalable and accommodative security for 5G/6G IoT systems. Moreover, examination and comparison of five machine learning models (XGBoost, random forest (RF), k-nearest neighbor (KNN), stochastic gradient descent (SGD), and naïve Bayes) for distributed denial of service (DDoS) detection and mitigation is delivered. While emphasizing the effectiveness of ML-based approaches, particularly XGBoost, for improving attack detection accuracy. Yet, the proposed framework may face challenges to optimize the computational overhead associated with AI/ML models to preserve transparency and trust in automated threat detection. Ullah and Mahmoud [39] introduces an anomaly-based intrusion detection model for IoT networks, utilizing convolutional neural networks in various dimensions. Validation using multiple datasets and transfer learning principles demonstrates high accuracy, precision, recall, and F1-score, surpassing existing deep learning implementations. Even though convolutional neural network (CNN)-based anomaly detection systems prompt significant computational overhead and demands extensive tuning.

The proposed federated-learning (FL)-based approach [40] employs on-device data for anomaly detection in IoT networks, preserving user privacy by sharing only learned weights. Utilizing gated recurrent units (GRUs) models and ensemble techniques, it achieves superior accuracy in attack detection compared to classic/centralized machine learning methods, as validated through experimental results. However, the solution requires enhancement and evaluation on IoT devices testbed to consider various IoT devices vulnerabilities. Yao *et al.* [41] provide a distributed system for intrusion detection to preserve security and privacy at the edge of IoT environments. The system uses a deep generative learning method to upgrade the accuracy and efficiency of detecting attacks. The experimental findings illustrate the efficiency of threat identification while preserving user privacy. Still, real-world deployment might face scalability challenges. Additionally, the complexity of deep generative models' may induce potential increase in computational overhead.

Lu *et al.* [42] develop a hybrid blockchain architecture and propose an asynchronous federated learning with deep reinforcement learning (DRL) for node selection. The solution improves efficiency, ensures shared data reliability through two-stage verification. Regardless, the limited feasibility assessments and real-world deployment make the practical deployment examination complex.

4. SUMMARY AND DISCUSSION

Table 2 provides a summary of the discussed research, outlining the main IoT applications and the security requirements covered for each contribution. The contributions cover a wide range of IoT applications, from smart home devices to connected cars and industrial IoT. A significant number of studies, such as those by [17], [19], address multiple application domains and security requirements, including privacy, scalability, and attack resistance. For example, Ali *et al.* [15] provides comprehensive coverage across all listed IoT applications and security requirements, emphasizing their broad applicability. In contrast, other studies focus on specific areas, such as privacy-preserving ML solutions by [34], [35], which are particularly relevant to smart city and healthcare IoT contexts. Notably, some contributions are tailored to specific needs, such as anomaly detection by [39], [40], which emphasize attack resistance and anomaly detection across multiple IoT applications. The analysis of ML-based solutions for privacy and/or confidentiality in IoT shows the triumph of federated learning and differential privacy for privacy-preserving IoT systems. Homomorphic encryption is very powerful for confidentiality but demands high computational cost. Meanwhile, generative AI and convolutional neural networks can be used with privacy-enhancing techniques. For anomaly detection and unauthorized access attempts, the combination of ML algorithms and zero-trust architecture ensures more robust security. Selecting a suitable ML algorithm depends on multiple factors as, data structure and real-time requirements. For secure data sharing and access control, reinforcement learning is greatest in dynamic IoT environments. Consequently, to create resilient privacy and confidentiality systems in IoT using machine learning, several recommendations can be considered: Federated learning adoption for distributed data processing, edge computing integration for local data processing, the use of differential privacy in ML models, and Blockchain for decentralized privacy management. Combine privacy by design with zero-trust architecture, robust mechanisms, and regulatory frameworks to ensure internet of things systems viability and efficiency.

Table 2. Summary of contributions in privacy and confidentiality in IoT environment

Contribution	IoT applications covered										Security requirements covered				
	Smart Home	Wearable Health	Smart City	Industrial IoT	Healthcare IoT	Smart Retail	Agriculture	Connected Cars	Environment	Energy	Privacy	Scalability	Authentication and Trust	End-to-End Security	Attack Resistant
Ali *et al.* [15]					√						√		√	√	√
Esfahani *et al.* [16]					√						√	√	√	√	√
Ali *et al.* [17]	√	√	√	√	√	√	√	√	√	√	√				
Abuladel *et al.* [18]					√						√		√		√
Xue *et al.* [19]	√	√	√	√	√	√	√	√	√	√	√				
Liu *et al.* [20]	√	√	√	√	√	√	√	√	√	√	√				
Wang *et al.* [21]									√		√				
Li *et al.* [22]			√			√					√				
Boussada *et al.* [23]					√						√				√
Gheisari *et al.* [24]			√								√				
Wang *et al.* [25]	√	√	√	√	√	√	√	√	√	√	√		√		√
Khashan and Khafajah [26]	√	√	√	√	√	√	√	√	√	√		√	√		√
Rashid *et al.* [27]	√	√	√	√	√	√	√	√	√	√			√		
Asif *et al.* [28]			√										√		
Hussain *et al.* [29]	√	√	√	√	√	√	√	√	√	√			√		√
Modu *et al.* [30]	√	√	√	√	√	√	√	√	√	√			√		
Apte *et al.* [31]	√	√	√	√	√	√	√	√	√	√			√		√
Sbaytri *et al.* [32]	√	√	√	√	√	√	√	√	√	√			√		
Zhu *et al.* [34]			√								√				
Bi *et al.* [35]					√						√				
Ullah and Mahmoud [39]	√	√	√	√	√	√	√	√	√	√					√
Mothukuri *et al.* [40]	√	√	√	√	√	√	√	√	√	√	√				√
Lu *et al.* [42]								√			√				

5. CONCLUSION

This paper has examined the critical issues surrounding privacy and confidentiality in the internet of Things through a detailed review of recent existing literature. The analysis of privacy-related work highlights the need for robust mechanisms to safeguard personal data against unauthorized access and misuse. In the realm of authentication and trust, it is evident that reliable and scalable solutions are essential to secure IoT environments. The review of machine learning-based approaches illustrates their potential to enhance privacy and confidentiality, offering advanced techniques for data protection and anomaly detection. Our findings suggest that, while significant progress has been made, there are still gaps and opportunities for further research. Future work should focus on developing integrated solutions that combine privacy-preserving techniques with advanced authentication and trust mechanisms, as well as leveraging emerging technologies to address evolving threats.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Hiba Kandil	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓
Hafssa Benaboud	✓	✓										✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

This study is based entirely on previously published data, which are available from the sources cited in the references section.

REFERENCES

[1] M. A. Husnoo, A. Anwar, R. K. Chakrabortty, R. Doss, and M. J. Ryan, "Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey," *IEEE Access*, vol. 9, pp. 153276–153304, 2021, doi: 10.1109/ACCESS.2021.3124309.

[2] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain," *ACM Computing Surveys*, vol. 53, no. 6, pp. 1–37, Nov. 2021, doi: 10.1145/3417987.

[3] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[4] E. Rodríguez, B. Otero, and R. Canal, "A survey of machine and deep learning methods for privacy protection in the internet of things," *Sensors*, vol. 23, no. 3, p. 1252, Jan. 2023, doi: 10.3390/s23031252.

[5] H. Yzzogh, H. Kandil, and H. Benaboud, "A comprehensive overview of AI-driven behavioral analysis for security in internet of things," in *The Art of Cyber Defense*, Boca Raton: CRC Press, 2024, pp. 40–51.

[6] J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives," *Computer Networks*, vol. 148, pp. 295–306, Jan. 2019, doi: 10.1016/j.comnet.2018.11.026.

[7] D. T. Aga, R. Chintanippu, R. A. Mowri, and M. Siddula, "Exploring secure and private data aggregation techniques for the internet of things: a comprehensive review," *Discover Internet of Things*, vol. 4, no. 1, p. 28, Nov. 2024, doi: 10.1007/s43926-024-00064-7.

[8] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, Aug. 2018, doi: 10.1016/j.comnet.2018.03.012.

[9] H. Kandil and H. Benaboud, "Using machine learning to deal with privacy and confidentiality in internet of things: An overview," 2025, pp. 774–783.

[10] M. binti Mohamad Noor and W. H. Hassan, "Current research on internet of things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.

[11] D. Mendez Mena, I. Papapanagiotou, and B. Yang, "Internet of things: Survey on security," *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 162–182, May 2018, doi: 10.1080/19393555.2018.1458258.

[12] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT threats: Survey of risks and vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, Oct. 2024, doi: 10.3390/fi16110389.

[13] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, Mar. 2019, doi: 10.3390/s19051141.

[14] D. Sey, "A survey on authentication methods for the internet of things," *PeerJ Preprints*, Jul. 23, 2018, doi: 10.7287/peerj.preprints.26474v2.

[15] A. Ali, B. A. S. Al-rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "HealthLock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications," *Sensors*, vol. 23, no. 15, p. 6762, Jul. 2023, doi: 10.3390/s23156762.

[16] M. Nasr Esfahani, B. S. Ghahfarokhi, and S. E. Borujeni, "Blockchain-based end-to-end privacy-preserving scheme for IoT-based healthcare systems," *The Journal of Supercomputing*, vol. 80, no. 2, pp. 2067–2127, Jan. 2024, doi: 10.1007/s11227-023-05522-7.

[17] W. Ali, M. Nauman, and N. Azam, "A privacy enhancing model for internet of things using three-way decisions and differential privacy," *Computers and Electrical Engineering*, vol. 100, p. 107894, May 2022, doi: 10.1016/j.compeleceng.2022.107894.

[18] A. Abuladel and O. Bamasag, "Data and location privacy issues in IoT applications," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, Mar. 2020, pp. 1–6, doi: 10.1109/ICCAIS48893.2020.9096837.

[19] W. Xue, W. Hu, P. Gauranvaram, A. Seneviratne, and S. Jha, "An efficient privacy-preserving IoT system for face recognition," in *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*, Apr. 2020, pp. 7–11, doi: 10.1109/ETSecIoT50046.2020.00006.

[20] Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, and J.-F. Xu, "Privacy-preserving raw data collection without a trusted authority for IoT," *Computer Networks*, vol. 148, pp. 340–348, Jan. 2019, doi: 10.1016/j.comnet.2018.11.028.

[21] H. Wang, G. Han, L. Zhou, J. A. Ansere, and W. Zhang, "A source location privacy protection scheme based on ring-loop routing for the IoT," *Computer Networks*, vol. 148, pp. 142–150, Jan. 2019, doi: 10.1016/j.comnet.2018.11.005.

[22] K. Li, L. Tian, W. Li, G. Luo, and Z. Cai, "Incorporating social interaction into three-party game towards privacy protection in IoT," *Computer Networks*, vol. 150, pp. 90–101, Feb. 2019, doi: 10.1016/j.comnet.2018.11.036.

[23] R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, "Privacy-preserving aware data transmission for IoT-based e-health," *Computer Networks*, vol. 162, p. 106866, Oct. 2019, doi: 10.1016/j.comnet.2019.106866.

[24] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Computers & Security*, vol. 87, p. 101470, Nov. 2019, doi: 10.1016/j.cose.2019.02.006.

[25] Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," *Future Generation Computer Systems*, vol. 82, pp. 342–348, May 2018, doi: 10.1016/j.future.2017.09.042.

[26] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 726–739, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.011.

[27] A. Rashid, A. Masood, and A. ur R. Khan, "Zone of trust: blockchain assisted IoT authentication to support cross-communication between bubbles of trusted IoTs," *Cluster Computing*, vol. 26, no. 1, pp. 237–254, Feb. 2023, doi: 10.1007/s10586-022-03583-6.

[28] M. Asif, Z. Aziz, M. Bin Ahmad, A. Khalid, H. A. Waris, and A. Gilani, "Blockchain-based authentication and trust management mechanism for smart cities," *Sensors*, vol. 22, no. 7, p. 2604, Mar. 2022, doi: 10.3390/s22072604.

[29] F. Hussain Al-Naji and R. Zagrouba, "CAB-IoT: Continuous authentication architecture based on blockchain for internet of things," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 2497–2514, Jun. 2022, doi: 10.1016/j.jksuci.2020.11.023.

[30] F. Modu, F. Aliyu, T. Sheltami, and M. Musa, "Energy-efficient multi-biometric system for internet of things using trust management," *IET Biometrics*, vol. 10, no. 6, pp. 625–639, Nov. 2021, doi: 10.1049/bme2.12028.

[31] M. Apte, S. Kelkar, A. Dorge, S. Deshpande, P. Bomble, and A. Dhamankar, "Gateway based trust management system for internet of things," *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 4, pp. 4750–4763, Aug. 2021, doi: 10.47059/revistageintec.v11i4.2501.

[32] Y. Sbaytri, S. Lazaar, H. Benaboud, and S. Bouchkaren, "A new secure cellular automata cryptosystem for embedded devices," 2019, pp. 259–267.

[33] Z. Ding *et al.*, "A Lightweight and secure communication protocol for the IoT environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 3, pp. 1050–1067, May 2024, doi: 10.1109/TDSC.2023.3267979.

[34] L. Zhu, X. Tang, M. Shen, F. Gao, J. Zhang, and X. Du, "Privacy-preserving machine learning training in IoT aggregation scenarios," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12106–12118, Aug. 2021, doi: 10.1109/JIOT.2021.3060764.

[35] H. Bi, J. Liu, and N. Kato, "Deep learning-based privacy preservation and data analytics for IoT enabled healthcare," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4798–4807, Jul. 2022, doi: 10.1109/TII.2021.3117285.

[36] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. K. M. N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Generation Computer Systems*, vol. 160, pp. 577–597, Nov. 2024, doi: 10.1016/j.future.2024.06.023.

[37] M. Shrestha, Y. Ravichandran, and E. Kim, "Secure multiparty generative AI," *arXiv preprint arXiv:2409.19120*, 2024.

[38] S. Shakya, R. Abbas, and S. Maric, "A novel zero-touch, zero-trust, AI/ML enablement framework for IoT network security," *arXiv preprint arXiv:2502.03614*, 2025.

[39] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[40] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, Feb. 2022, doi: 10.1109/JIOT.2021.3077803.

[41] W. Yao, H. Zhao, and H. Shi, "Privacy-preserving collaborative intrusion detection in edge of internet of things: a robust and efficient deep generative learning approach," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15704–15722, May 2024, doi: 10.1109/JIOT.2023.3348117.

[42] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020, doi: 10.1109/TVT.2020.2973651.

BIOGRAPHIES OF AUTHORS

Hiba Kandil received her master's degree in computer science from the Faculty of Sciences, Mohammed V University in Rabat, Morocco, in 2016. She is currently pursuing a Ph.D. at the same university. Her research interests include the internet of things (IoT), security, network security, machine learning, and deep learning. She can be contacted at email: hiba_kandil@um5.ac.ma.

Hafssa Benaboud received her Ph.D. degree in computer science from the University of Burgundy in Dijon, France, in 2004. In 2005, she joined the National School of Applied Sciences (ENSA) of Tangier, Morocco, as an assistant professor. Since 2011, she has been serving as a full-time professor in the Department of Computer Science at Mohammed V University in Rabat, Morocco. She has authored more than 30 articles published in international journals and conference proceedings. Her research interests include network protocols, network security, the internet of things, traffic analysis, and quality of service. She can be contacted at hafssa.benaboud@fsr.um5.ac.ma.