frontiers | Frontiers in Computer Science

TYPE Review
PUBLISHED 26 June 2024
DOI 10.3389/fcomp.2024.1420680

OPEN ACCESS

EDITED BY
Arslan Musaddiq,
Linnaeus University, Sweden

REVIEWED BY
Raman Singh,
University of the West of Scotland, United Kingdom
Bishwajeet Kumar Pandey,
Astana University, Kazakhstan

*CORRESPONDENCE
Kawalpreet Kaur
✉ kaur.kawalpreet17@gmail.com
Yonis Gulzar
✉ ygulzar@kfu.edu.sa

RECEIVED 20 April 2024
ACCEPTED 12 June 2024
PUBLISHED 26 June 2024

CITATION
Kaur K, Kaur A, Gulzar Y and Gandhi V (2024) Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies.
Front. Comput. Sci. 6:1420680.
doi: 10.3389/fcomp.2024.1420680

Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies

Kawalpreet Kaur[1,2]*, Amanpreet Kaur[1], Yonis Gulzar[3]* and Vidhyotma Gandhi[4]

[1]Chitkara Institute of Engineering and Technology, Chitkara University, Punjab, India, [2]Goswami Ganesh Dutta Sanatan Dharma College, Chandigarh, India, [3]Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa, Saudi Arabia, [4]Gyancity Research Labs, Gurugram, India

The Internet of Things (IoT) is a collection of devices such as sensors for collecting data, actuators that perform mechanical actions on the sensor's collected data, and gateways used as an interface for effective communication with the external world. The IoT has been successfully applied to various fields, from small households to large industries. The IoT environment consists of heterogeneous networks and billions of devices increasing daily, making the system more complex and this need for privacy and security of IoT devices become a major concern. The critical components of IoT are device identification, a large number of sensors, hardware operating systems, and IoT semantics and services. The layers of a core IoT application are presented in this paper with the protocols used in each layer. The security challenges at various IoT layers are unveiled in this review paper along with the existing mitigation strategies such as machine learning, deep learning, lightweight encryption techniques, and Intrusion Detection Systems (IDS) to overcome these security challenges and future scope. It has been concluded after doing an intensive review that Spoofing and Distributed Denial of Service (DDoS) attacks are two of the most common attacks in IoT applications. While spoofing tricks systems by impersonating devices, DDoS attacks flood IoT systems with traffic. IoT security is also compromised by other attacks, such as botnet attacks, man-in-middle attacks etc. which call for strong defenses including IDS framework, deep neural networks, and multifactor authentication system.

KEYWORDS

IoT, IoT applications, IoT layers, mitigation strategies, network and communication protocols, security challenges

1 Introduction

Connected devices and Internet usage are increasing worldwide, mostly in North America, west Europe, and China (Kandaswamy and Furlonger, 2018). In 2024, machine-to-machine communication will grow to 27 billion instead of 5.6 billion in 2016 (Kandaswamy and Furlonger, 2018). Therefore, IoT is considered one of the prime forthcoming markets that will greatly affect the digital economy. In terms of revenue, the IoT industry is expected to reach $4 trillion by 2025, a huge number. IoT has a vast number of applications whether

machine-to-human or machine-to-machine communication in health trackers, smart retail, smart cities, and smart grids (Fernández-Caramés and Fraga-Lamas, 2018). Figure 1, displays the building blocks of IoT. The basic components of IoT include smart objects for collecting data, and the exchange of data is done through Wifi or Bluetooth. Smart analytics can be done by using cloud services and various technologies such as Wireless Sensor Networks (WSN), cloud computing, edge computing, fog computing, and machine learning are integrated. The interaction of data is possible through machine-to-machine, human-to-machine, and machine-to-human, and communication is done in any network whether it is homogeneous or heterogeneous.

Earlier IoT devices were used to communicate through the cloud, where all the information is stored in the cloud only. Nowadays, fog and edge computing are also used with cloud computing to increase the computation speed and solve complex problems (Ahanger et al., 2022). In the future, direct communication between devices on the Internet will be possible. IoT applications collect a lot of user data and store it at various nodes before and after processing.

Ensuring the confidentiality, integrity, and availability of IoT data faces several challenges (Schiller et al., 2022). In the intricate tapestry of the IoT, data security emerges as a paramount concern at the heart of this interconnected realm. As the IoT generates a staggering volume of sensitive information, safeguarding its integrity becomes a daunting task. Numerous challenges arise, encompassing the specter of unauthorized access, privacy breaches, and data manipulation (Koohang et al., 2022; Sarker et al., 2023). To address these challenges, robust mitigation strategies must be implemented.

This paper aims to examine the variety of security risks that affect IoT devices, as well as the attack types. This paper intends to investigate and assess different approaches and solutions that could be used to mitigate these risks, with an emphasis on improving the security of IoT systems. These include, but are not restricted to, malware, data breaches, and Denial of Service (DoS) attacks. The study also aims to investigate current security protocols used in IoT systems and evaluate how well they work to counter new threats. This paper has 10 sections organized as follows: In Section 2, the research methodology is fully elaborated. Section 3 provides an overview of IoT and the current state of IoT security. Section 4 is dedicated to the literature review of previous works. In Section 5, IoT layers are explained along with the protocols used in various layers. Section 6 examines the security threats faced by each layer of the IoT architecture. It will identify security attacks associated with each layer and discuss their potential impact on IoT systems. Section 7 reviews current security solutions and countermeasures. Then, in Section 8 discussion is presented. Finally, in Section 9, the conclusion is presented with the possibility of future work.

1.1 IoT security

The major concern here is how to protect this data from intruders or hackers who are always keen to access a user's private data, as the Internet and other networks are still facing security problems. IoT has its own security and privacy issues such as device authentication, management, processing, and storage issues, etc. IoT devices have limited storage capacity, so heavy security measures cannot be incorporated. Only lightweight algorithms are preferred (Hassija et al., 2019). Besides this, IoT devices are using heterogeneous devices over diverse networks so they are more vulnerable to attacks. There have been numerous privacy and security attacks on IoT data and applications. According to the Healthcare Data Breach Trend Report 2021. Recent data shows that the frequency of malicious attacks and illegal disclosure of healthcare data has risen tremendously in the last 3 years" (H1 Healthcare Data Breach Report, 2022).

The two security incidents were reported by "Ring. an Amazon-owned company. One was due to third-party trackers accidentally embedded in their Android application disclosing private information to social networking websites and another incident took place in smart homes where hackers monitored the homes of many families (IoT Security Breaches, 2022). Due to the usage of default usernames and passwords, cybercriminals could not only access live CCTV footage from smart homes but were able to operate these devices remotely. The 30 members of 15 families were persecuted in person by cybercriminals for misusing IoT sensor devices. In May 2019, an Internet security company, Applied Risk, spotted 10 security breaches in IoT devices by which, after stealing user IDs and passwords, cybercriminals can operate home security locks, install software and even a DoS attack can be launched. All attacks are carried out by breaking security measures at the place of service (IoT Security Breaches, 2022). IoT applications rely on interconnected devices that require security, such as smart cameras and medical devices, while internet connectivity enables data exchange and access to cloud-based services as shown in Figure 2.

The attackers make use of IoT devices for their bots so that they can attack specific websites or even whole networks with heavy traffic and halt the IoT system for their use. The botnet attacks are affecting more than 35% of smart homes globally as published in the Gartner report (Internet of Things, 2022). If the whole botnet is controlled by attackers in turn controlling a vast number of smart home devices enables hackers to impair the whole power system (Botnets Latest News, Photos and Videos WIRED, 2022).

Abbreviations: AEs, Autoencoders; AMQP, Advanced Message Queuing Protocol; AODV, *Ad-hoc* On-demand Distance Vector; APT, Advanced Persistent Threat; CNN, Convolutional neural network; CoAP, Constrained Application Protocol; DCNN, Distributed Convolutional Neural Network; DDoS, Distributed Denial of Service; DDS, Data Distribution Service; DODAG, Directed Acyclic Graph; DoS, Denial of Service; ECC, Elliptic Curve Cryptography; FCM, fuzzy C-means; FDI, False Data Injection; FPGA, Field Programmable Gate Array; HMAC, Hash Message Authentication Code; HTTP, Hypertext Transfer Protocol; IDS, Intrusion Detection Systems; IoT, Internet of Things; ISHO, Improved Spotted Hyena Optimization; LSH, Locality Sensitive Hashing; LSTM, Long Short-Term Memory; MP2P, MultiPoint-to-Point; MQTT, Message Queue Telemetry Transport Protocol; OWASP, Open Web Application Security Project; P2MP, Point-to-MultiPoint; P2P, Point-to-point; PAN, Personal area network; PCA, Principal Component Analysis; PUF, Physical Unclonable Functions; RFID, Radio Frequency Identification; RPL, Routing Protocol; RSSI, Received Signal Strength Indication; SCA, Side Channel Attacks; SGX, Software Guard Extensions; SOAP, Simple Object Access Protocol; SRAS, Secure Return Address Stack; SSL, Secure Socket Layer; SVM, Support Vector Machine; TLS, Transport Layer Security; WFL, Weighted Federated Learning; WSN, Wireless Sensor Networks; XMPP, Extensible Messaging and Presence Protocol.

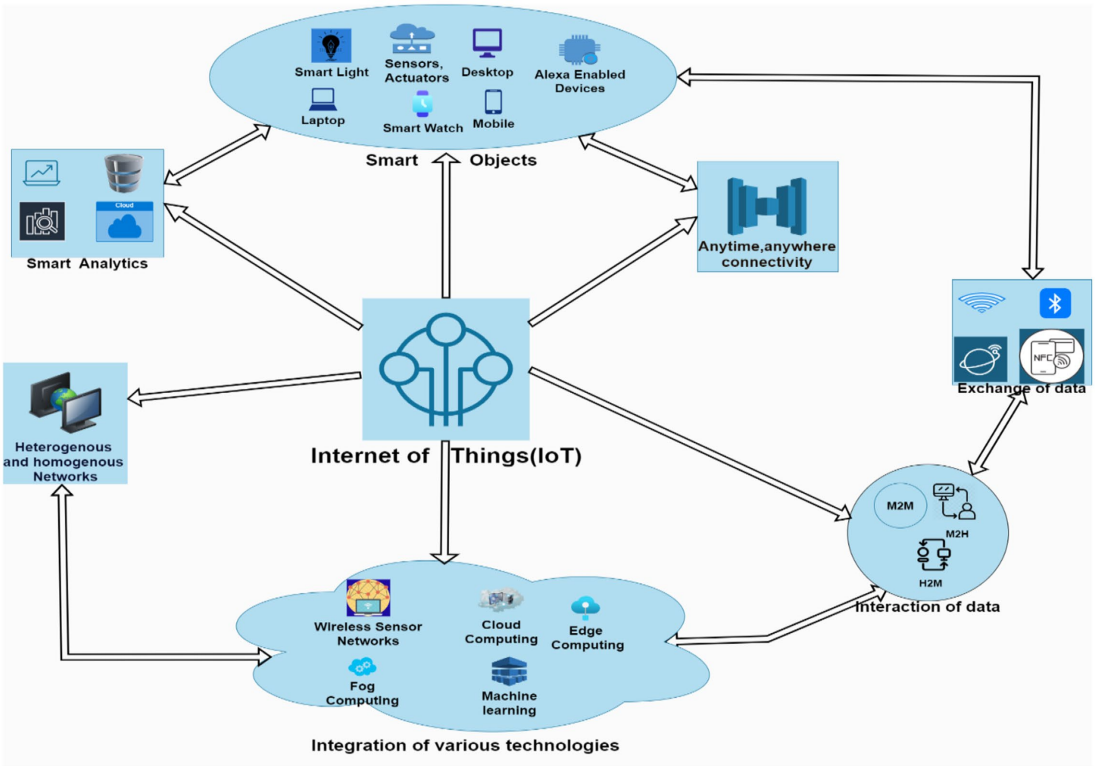

FIGURE 1
Internet of Things.

2 Methodology

In this article we have followed a process which is based mainly on two main parts firstly search and then review. In the first process, maximum effort is put into finding keywords related to IoT like

- "IoT protocols"
- "IoT layers"
- "IoT data security attacks"
- "IoT security solutions and mitigation strategies".

These keywords are selected as it covers all the topics strated from IoT in general and then going toward the details of IoT layers, security attacks and solutions. From all the articles retrieved, articles that are related to this study have been shortlisted. This process was based on the review of more than 300 published and reviewed papers related to IoT. The Prisma flow diagram is shown in Figure 3, depicts the process of systematic review conducted in this study.

The methodology for the review paper on IoT data security attacks and mitigation strategies can be outlined as follows:

2.1 Search criteria

- Identify relevant keywords and phrases related to IoT data security attacks and mitigation strategies.
- Utilize reputable academic databases, such as IEEE Xplore, Scopus, SCI, and Google Scholar.
- Consider recent publications from 2018 to 2023 to ensure the inclusion of up-to-date information.
- Include articles, conference papers, and whitepapers that address IoT security attacks and propose solutions.

2.2 Inclusion criteria

- Include articles that specifically focus on IoT data security attacks, vulnerabilities, or threats.
- Include articles that propose or discuss solutions, countermeasures, or mitigation techniques for IoT security attacks.
- Include studies that evaluate the effectiveness of existing solutions or propose new methodologies to enhance IoT security.
- Include articles that cover various layers of the IoT architecture, such as device, communication, network, and application layers.

2.3 Exclusion criteria

- Exclude articles that do not directly address IoT security attacks or propose solutions.
- Exclude articles that are not peer-reviewed or lack credible sources.
- Exclude articles that are not written in English.

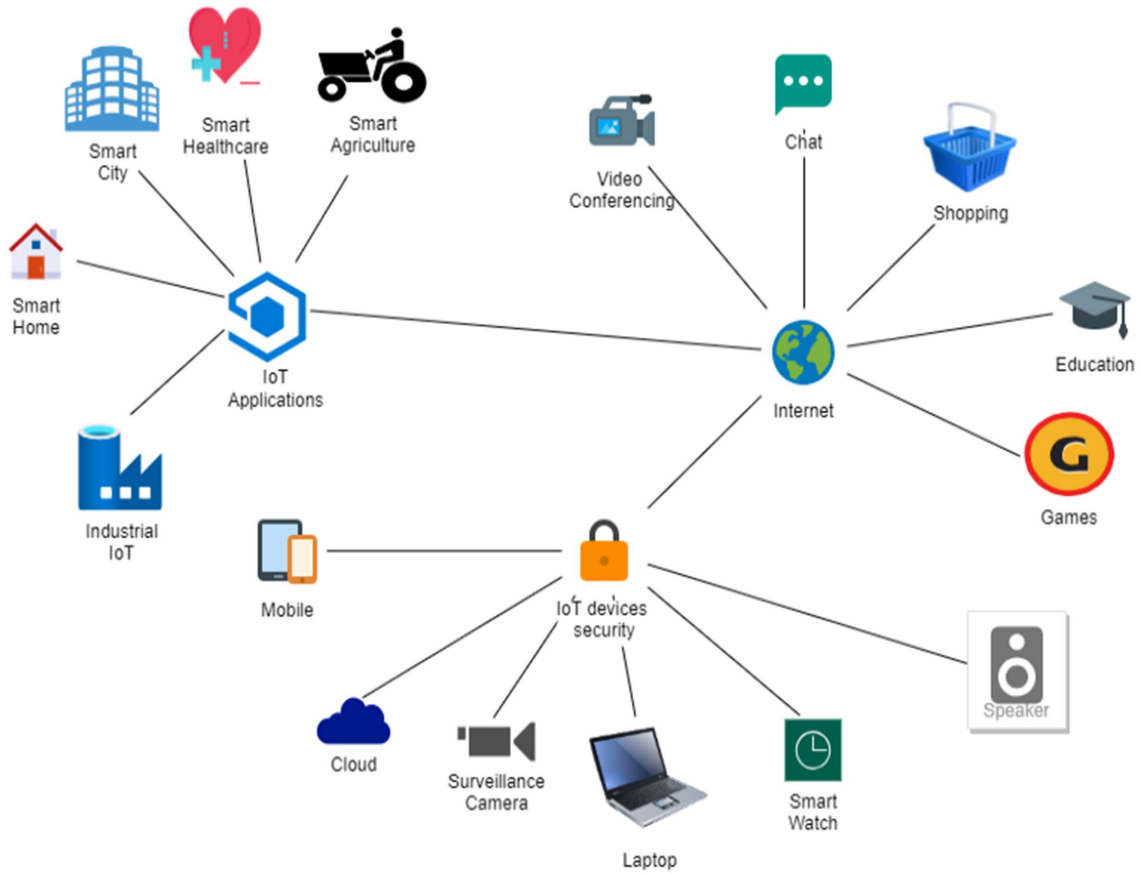

FIGURE 2
Unleashing the power of IoT: safeguarding a connected future.

2.4 Screening process

- Conduct an initial screening of titles and abstracts to identify potentially relevant articles
- Apply inclusion and exclusion criteria to further refine the selection of articles.
- Review full-text articles that pass the initial screening to determine their suitability for inclusion.
- Resolve any discrepancies through consensus among the authors.

2.5 Data extraction

- Extract relevant information from the selected articles, such as research objectives, methodologies, attack types, and proposed solutions.
- Systematically organize the extracted data for analysis and discussion.

2.6 Analysis and synthesis

- Analyze the collected data to identify common trends, patterns, and challenges in IoT security attacks and solutions.
- Compare and contrast different approaches and methodologies proposed in the literature.
- Summarize the findings and provide a comprehensive overview of the current state-of-the-art in IoT security attacks and solutions.

A total of 356 articles related to IoT in security were identified from the database, out of which 226 articles did not meet the inclusion criteria and were excluded from the study.

3 Roadmap of IoT to the IoT security in the state of art

Table 1 shows how IoT technology has evolved over time and how it's become more secure. At first, IoT devices connected without much protection. But as IoT grew, people realized the need for better security. This path illustrates the transition from basic security to the current strong emphasis on IoT security.

Figure 4, depicts a significant amount of research and development in the field of IoT technology. However, it also underscores that the progress in IoT security measures has been comparatively limited, with ongoing efforts to enhance security in this domain. Figure 5 (Dimensions), provides a chronological (starting from 2018) overview of the increasing volume of publications related to the IoT. This journey showcases how IoT

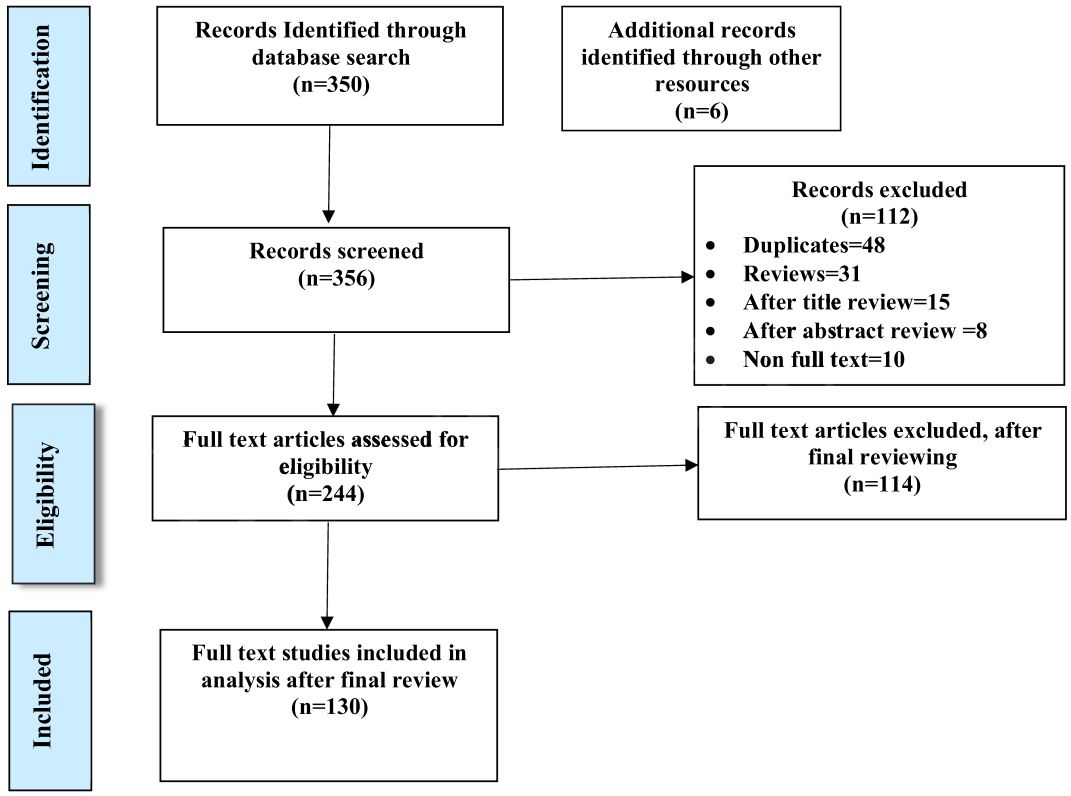

FIGURE 3
Prisma flow diagram for literature review on IoT security.

TABLE 1 From IoT to IoT security: a progression toward protection.

Strings	IEEE explore	Google scholar	ACM digital library	Mdpi	Springer	Taylor and Francis
IoT	75,985	87,400	19,555	25,103	88,912	6,116
IoT AND applications	34,524	71,900	18,669	22,643	81,145	5,816
IoT AND applications AND security	9,669	77,100	10,570	12,989	47,791	3,303
IoT AND (applications OR layers) AND security	1,214	67,200	10,671	12,017	33,632	3,346
IoT AND (applications OR layers or protocol) AND security	466	17,800	10,671	14,433	22,886	3,357
IoT AND (applications OR layers and protocol) AND (security or security attacks)	162	18,000	10,985	14,515	14,588	1,159
IoT AND (applications OR layers and protocol) AND (security or security attacks or mitigation strategies OR security solution)	45	17,800	16,697	15,278	4,822	1,508

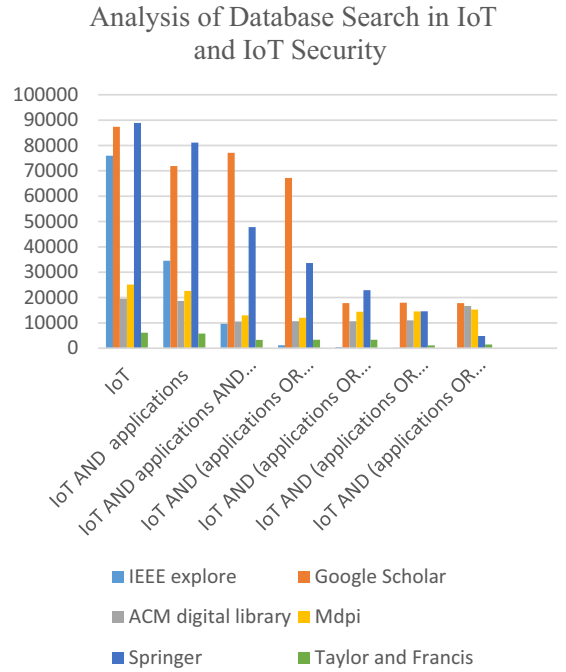

FIGURE 4
Database dive: unraveling IoT and security database search.

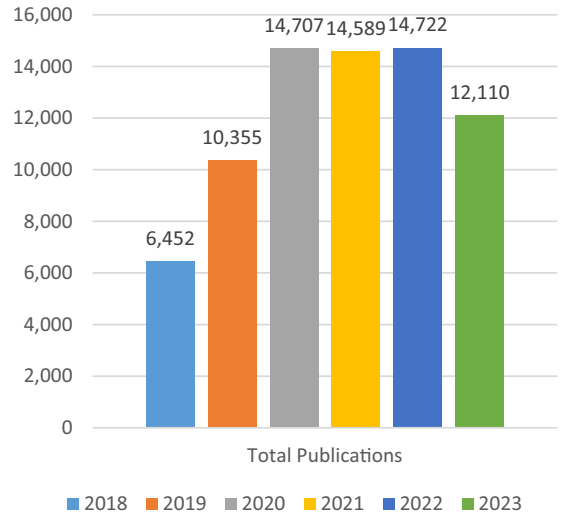

FIGURE 5
IoT's rising tide: a year wise publication journey.

research and literature have grown over time, capturing the rising interest and insights into this field over the years.

Figure 6 (Dimensions), is a depiction of the evolution of security measures within the IoT domain. It serves as a historical record of how the protection of IoT devices and data has progressed and adapted to emerging threats.

The chart shows a strong dedication to strengthening digital security over time, offering a full picture of IoT security's progress. In addition to the progress shown above, there is still much work to

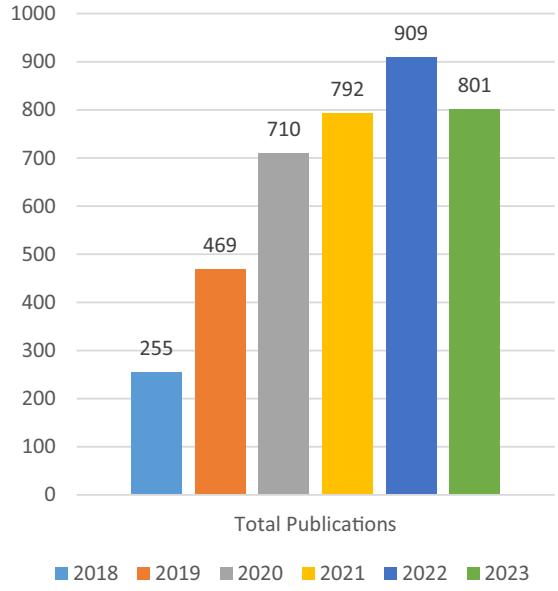

FIGURE 6
Guardians of the digital realm: IoT security over the years.

be done in the field of IoT security to ensure safety against emerging cyber threats.

4 Literature review

The literature review regarding IoT security is described in Figure 7, concerning the most widely used IoT applications:

4.1 IoT security

The major challenge that is being faced today is the security of these devices. The security of these devices is violated for many reasons, but one of the prime reasons is storing data with default, weak, or no passwords at all (Internet of Things Report, 2022). That gives the hacker easier access to the user's confidential data and by using this data, DDoS attacks can be launched on the IoT network, which can halt the whole IoT system. The large scale Mirai attack in 2016 was due to the default password stored in IoT systems (Kolias et al., 2017). The other reason for security violations of IoT devices is that they run on less power, low encryption methods, and limited resources, and storage (Ahemd et al., 2017; Aydos et al., 2019). The various security attacks identified by Ahmad and Alsmadi (2021) and the recent literature review have been provided with limitations. A three-stage approach has been applied to protecting IoT systems. First, firewalls are implemented to filter new traffic. Second, intrusion detection systems are implemented to detect the vulnerabilities that penetrate the firewall.

Last, a recovery system is implemented so that the IoT system can respond quickly when an IDS alarm is hit, indicating that security has been breached. Mostly, large-scale attacks are launched by compromising millions of IoT devices to create a botnet. Botnets are

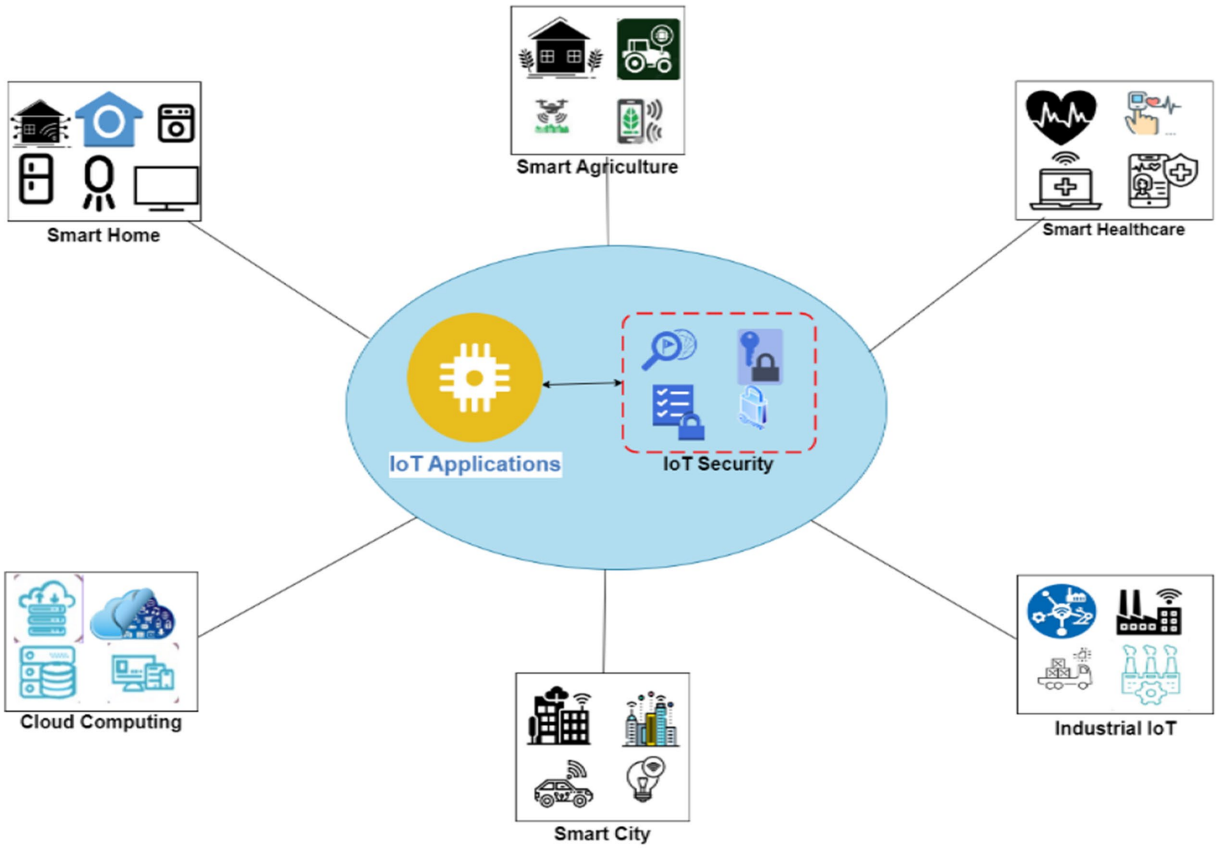

FIGURE 7
IoT applications keeping in view security as a key factor.

used to launch DDoS attacks that consume the entire bandwidth and resources of the target system. Because of the resource constraint problem of IoT devices, edge data centers are used to implement deep learning models for security. But still, there are a lot of issues with these approaches that need to be solved to enjoy the full benefit of these techniques (Ahmad and Alsmadi, 2021).

The IoT is based upon Radio Frequency Identification (RFID) and WSN as well as protocols and standards needed to support device-to-device communication. As IoT devices are collecting large data from heterogeneous networks and these devices have low storage capacity and high installation costs, a lot of other security issues in terms of data storage, cloud, big data, and RFID are discussed. Tewari and Gupta (2020) also described the efforts of IoT in various industries.

IoT is the most widely used technology in modern applications. The smart things connected to the IoT environment capture information and corresponding action is done. Mohanta et al. (2020) described an IoT infrastructure with protocols defined in each layer. The application areas of IoT and various security issues are identified. To address security issues, three main technologies, namely machine learning, artificial intelligence, and blockchain, are studied.

IoT is connected to two things, which are data and connectivity. So, it is important to secure data generated by IoT systems and various data transmission channels. Mohanty et al. (2021) described IoT architecture as 3 layered physical, network, and application. Layer-wise security issues and their possible solutions are discussed, as protocols are the backbone of any communication, layer-wise protocols, and their security mechanism are discussed.

An IoT environment consists of heterogeneous networks and billions of devices increasing day by day, making the system more complex and this need for privacy and security of IoT devices becomes a major concern. The critical components of IoT are device identification, various sensors, hardware operating systems, and providing semantics and services for IoT. The security at each layer is crucial but Khattak et al. (2019) discussed the security at the perception layer by using two main key technologies, RFID and Wireless sensor networks. The perception layer is the point where data is collected from the external environment. The layer-wise security attacks in the context of RFID and sensor networks and their possible solutions are discussed. These attacks have significant implications for IoT applications (Rani et al., 2020), ranging from data breaches and privacy violations to disruptions in critical services and potential physical harm in sectors such as healthcare, smart.

home, smart city, cloud computing, smart agriculture, and industrial automation (Savithri et al., 2022) as shown in Figure 8.

In an IoT network, data collection is done by sensors. Microcontrollers such as Arduino, and Raspberry Pi are used to process that data, stored in the cloud for future use, and analysis is done by any tool or language. Today, IoT has been applied in prime areas such as healthcare, industry, and smart city applications. The security of IoT devices is as important as the data communication process. For effective communication to take place, it is vital to secure the whole IoT network. This can be achieved with the help of protocols

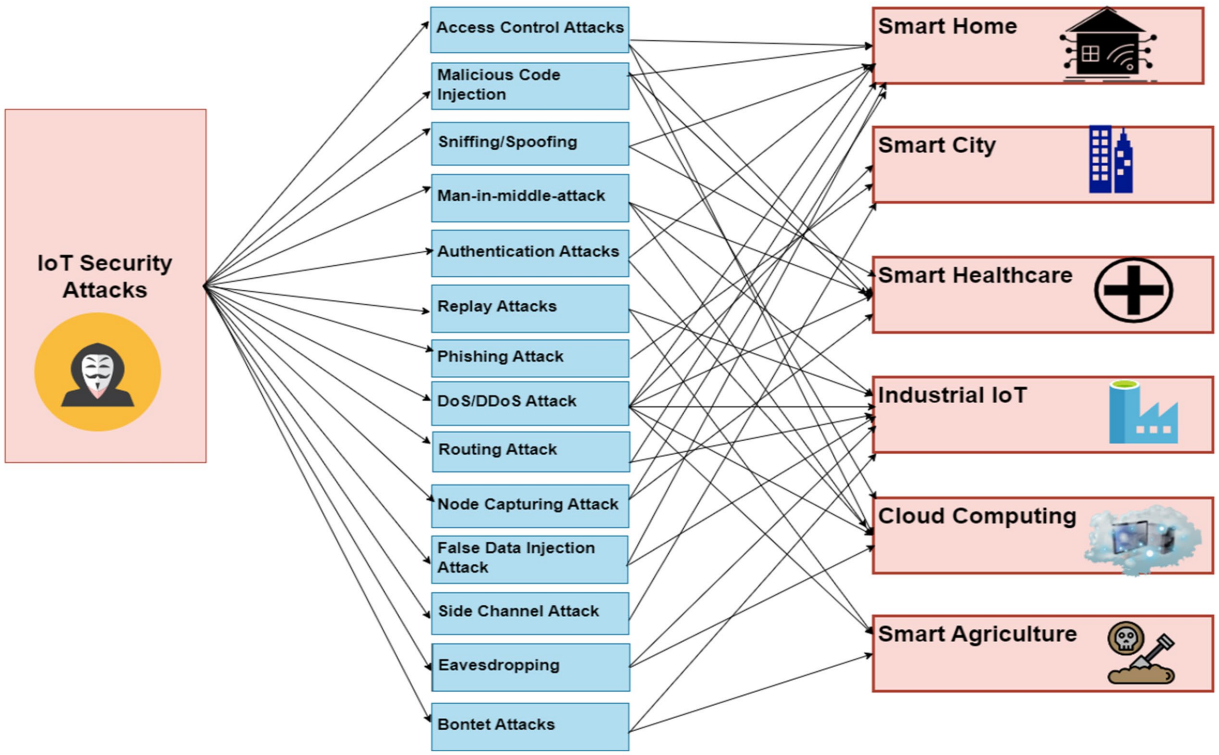

FIGURE 8
Overview of IoT security attacks and their impact on applications.

as they are the backbone for any communication to take place. However, IoT protocols work with IP protocols to provide effective transmission. The user data is exposed to various threats and attacks, therefore a standardization of IoT devices is required at the manufacturing level. The various IoT security issues along with requirements are discussed. The layer-wise IoT security protocols, their issues, and solutions are identified by Cynthia et al. (2019).

Yugha and Chithra (2020) discussed IoT layered architecture with layer-wise protocols. IoT security issues are discussed layer-wise and various IoT implementation tools are described in healthcare studies. Noor and Hassan (2019) identified layer-wise IoT security issues, mainly data security and privacy that arise because of heterogeneous IoT devices and networks. The two main IoT security solutions have been discussed. Those are authentication and encryption, but both solutions still need a lot of improvement to provide secure communication.

The different IoT devices are being connected to impart smart facilities to the user. As devices are different, there is a need to protect IoT data at various access points. For this reason, IoT is clubbed with various machine learning methods to provide secure, authenticated data and make offloading of data more authentic (Xiao et al., 2018). The main threat in IoT data transmission is data security, so Safi (Safi, 2017) suggested a hybrid encryption method to reduce data privacy risk. It has also been shown through MATLAB that this encryption technique has better speed when used with a digital signature.

IoT security attacks encompass a range of malicious activities aimed at exploiting vulnerabilities in IoT devices, networks, or applications. These attacks include device exploitation, botnets, eavesdropping, sleep deprivation attacks, phishing sites, and sniffing attacks (Noor and Hassan, 2019). To mitigate these risks, strong authentication, encryption, regular updates, network segmentation, and security monitoring are essential. Besides these, various solutions are given by authors such as IDS, Field Programmable Gate Array (FPGA), Improved Spotted Hyena Optimization (ISHO) algorithm, and various machine learning models as described in Table 2. By implementing robust security measures, organizations and individuals can safeguard against IoT security attacks and ensure the integrity and privacy of IoT systems and data.

4.2 Healthcare

To improve the security in medical IoT Jyotheeswari and Site (2020) suggested a security model using SHA-256 and AES-256 algorithms using an advanced encryption standard that is used in OpenSSL. This proposed algorithm has decreased the overhead incurred in the encryption and decryption computation process and also improved the performance. A person's heartbeat can be used to anticipate a person's fitness concerning their age. The stress levels of a person can be determined by monitoring the heart rate of the person so that patients get notified in case of some severe condition. The IoT and machine learning are working together to achieve this as, with the help of supervised learning, patient conditions can be foreseen and IoT is useful in communicating. The machine learning algorithm works well for authentic data (Selvaraj and Sundaravaradhan, 2020).

Security attacks can include unauthorized access to medical devices, manipulation of patient data, disruption of critical healthcare services, DoS attacks, man-in-middle attacks, and even the potential for physical harm as shown in Table 3. For example, a compromised IoT device could provide incorrect readings or dosages, leading to

TABLE 2 IoT security attacks: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
Xu et al. (2016)	Eavesdropping and interference	Relay transmission	Little performance loss
Bhattasali and Chaki (2011)	Sleep deprivation attacks	Lightweight multilayer IDS	Effective only in a simulated environment
Tufts University and IEEE Circuits and Systems Society (2017)	Booting attacks	FPGA	ZC706-based IoT device not secure
Sabahno and Safara (2021)	Phishing site attack	ISHO algorithm	Not examined on the real data set and phishing website detection.
Kiran et al. (2020)	Sniffing attacks	Machine learning models	Security features are not considered in the design process.
Liu and Du (2023)	Botnet attacks	Feature selection method based on a genetic algorithm	Class imbalance problems

TABLE 3 IoT security attacks on smart healthcare: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
Fotouhi et al. (2020)	Node capturing	Authentication protocol	Not applied in the real environment
Salem et al. (2022)	Man-in-the-middle attack	Framework using locality sensitive hashing (LSH) and HMAC	Not suited for other attacks like jamming or channel-hoping attacks
Chaudhry et al. (2021)	Access control attack	ECC	Increased computational cost
Jabeen et al. (2023)	Malicious node attacks	Genetic-based algorithm	Less effective
Vijayakumar et al. (2023)	ARP spoofing and DoS attacks	A deep neural network-based cyber-attack detection system	Less scalability and not tested in a real-time environment
Fontanella et al. (2023)	Man-in-the-middle attack	Architecture over the communication layer that offers mutual authentication	Weak security

TABLE 4 IoT security attacks on the smart city: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
IEEE Signal Processing Society (2018)	Side channel attacks	Packet obfuscation scheme	Creating extra delay
Velliangiri et al. (2023)	DoS attack	Attack detection model	–
Sangaiah et al. (2022)	Sinkhole attack	Clustering Multi-Layer Security Protocol (CL-MLSP) with *Ad-hoc* On-demand Distance Vector (AODV)	–
Vijayakumar et al. (2023)	Phishing attack	Real-time framework inspired by the honeybee defense mechanism	Improve the method of investigating the URL content
Sousa et al. (2023)	Flooding attack	IDS using machine learning algorithms	Not applicable in platooning scenarios

misdiagnosis or improper treatment (Ben Othman et al., 2022). To address these threats, robust security measures such as device authentication, data encryption, Hash Message Authentication Code (HMAC) (Salem et al., 2022), and Elliptic Curve Cryptography (ECC) (Chaudhry et al., 2021), etc. are identified.

4.3 Smart city

The smart city is one of the major applications of IoT, but it suffers from some issues such as data privacy, security, and confidentiality (Kouicem et al., 2018). Therefore Chen et al. (2021) suggested an artificially intelligent model based on Big Data that uses a differential algorithm to overcome the various security issues in smart city applications. IoT is the modern nature of communication as it is used to transmit data between different devices. Jindal et al. (2019) discussed the smart city application of the IoT and various machine learning algorithms that can be applied with IoT to achieve better and more accurate results.

Smart city systems, which integrate various IoT devices and technologies, are vulnerable to several attack vectors. For instance, malicious actors may target the city's sensor networks, transportation systems, or energy grids to disrupt operations or cause widespread damage. Attacks such as data breaches, unauthorized access, side channels, sinkholes, phishing, flooding attacks, or even ransomware attacks can compromise the integrity, availability, and confidentiality of sensitive information. Smart city initiatives as described in Table 4 must prioritize robust security measures, including secure

TABLE 5 IoT security attacks on smart home: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
Kasinathan et al. (2013)	DDoS/DoS attack	IDS framework	Unable to detect complex attacks.
Santos et al. (2019)	Routing attacks	IDS using Clustering and Reliability modules	A single model is not used to detect multiple routing attacks.
Kesswani and Agarwal (2020)	Spoofing and sniffing attacks	RFID-enabled multifactor authentication model	Extra overhead and model are not practically implemented
Khanpara et al. (2023)	Device hijacking, and unauthorized access	Context-aware security-based scheme	–
Cho et al. (2022)	Device capture attacks	Secure user authentication scheme using Physical Unclonable Functions (PUF)	Not suitable for practical smart homes

TABLE 6 IoT security attacks on cloud computing: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
Telo (2023)	Malware attacks	Multi-factor authentication	–
Sivasankari and Kamalakkannan (2022)	Man-in-middle-Attack	Regression modeling	–
Ali et al. (2023)	DDoS Attack and Low-Rate DDoS (LR-DDoS)	Weighted Federated Learning (WFL)	Not applied in the real-time network environment
Wu et al. (2022)	Eavesdropping	Intel Software Guard Extensions (SGX) based authentication key agreement protocol	Computational cost is slightly higher
Wu et al. (2022)	Authentication attacks	Lightweight Centralized Authentication Mechanism	Increased Computational and storage overhead

communication protocols, encryption, access controls, real-time framework (Vijayakumar et al., 2023), IDS (Sousa et al., 2023), and effective attack detection models (Velliangiri et al., 2023) to mitigate the risks associated with IoT security attacks and safeguard the city's infrastructure and citizens' privacy (Kumar et al., 2021).

4.4 Smart home

As the need for technology upgrades is rising, it is also required to protect and secure IoT data in smart homes (Song et al., 2017). To make this possible, a lightweight blockchain model is proposed. Mohanty et al. (2020) carried out three schemes for optimization and deployed this model into the smart home environment.

IoT security attacks can exploit vulnerabilities in the connected devices and networks within a smart home ecosystem. One common attack is unauthorized access, where malicious actors gain control over smart devices like cameras, door locks, or thermostats. This intrusion can lead to privacy breaches and unauthorized surveillance of residents. Another threat is the injection of malicious code into the system, allowing attackers to manipulate or disable smart home functionalities. Additionally, false data injection attacks can result in incorrect readings or actions by the devices, impacting the efficiency and reliability of automated tasks (Hammi et al., 2022). Smart homes are also vulnerable to other attacks, such as DoS, routing, spoofing, or even device capture attacks as mentioned in Table 5. Therefore, smart home users must implement strong security measures, including the IDS framework (Kasinathan et al., 2013; Santos et al., 2019), and user authentication mechanisms (Kesswani and Agarwal, 2020; Cho et al., 2022), to safeguard against these potential threats.

4.5 Cloud computing

IoT data is stored in the cloud for further processing and analysis. Therefore, cloud computing has prime importance in storing and maintaining IoT data. Yan et al. (n.d.) suggested an efficient attribute-based encryption method with cryptography based on pairing to deduplicate IoT encrypted data so that secure data access can be provided in case of confidential data transmission.

IoT security attacks on cloud computing pose significant risks to the confidentiality, integrity, and availability of data and services. One of the major concerns is the unauthorized access to sensitive information stored in the cloud. Another common attack is the injection of malicious code into cloud applications or services, man-in-middle-attacks or even eavesdropping, allowing attackers to manipulate data or compromise the functionality of the system. Additionally, DDoS attacks can disrupt cloud services, causing downtime and affecting the availability of IoT applications (Ahmad et al., 2022). Mitigating these risks requires implementing robust security measures such as encryption, lightweight access control mechanisms (Wu et al., 2022), regression modeling (Sivasankari and Kamalakkannan, 2022), federated learning (Ali et al., 2023), and ensuring the use of trusted and secure cloud service providers as outlined in Table 6.

TABLE 7 IoT security attacks on Industrial IoT: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
Aboelwafa et al. (2020)	False data injection attack	Autoencoders(AEs)	Vulnerability to Correlated Attacks
Yavuz et al. (2018)	Routing attack	Deep-learning-based machine learning method	Multiple models are used.
Jing and Wang (2022)	DDoS attack	Principal Component Analysis (PCA)- fuzzy C Means (FCM) clustering Model	Not accurate and fast enough to detect all DDoS attacks.
Kumar Donta et al. (2023)	Botnet attack	Real-time network environment	Not applied in publicly available datasets
Yang et al. (2023)	Replay attacks, Eavesdropping attacks, Man-in-the-middle attacks, and simulated attacks	ECC and trusted tokens with packet encryption using the TLS protocol	Complicated authentication process on terminal devices

TABLE 8 IoT security attacks on smart agriculture: solutions and limitations.

Ref. No.	Attack	Solution	Limitation
Aldhyani and Alkahtani (2023)	DDoS attack	Convolutional neural network combined with long short-term memory (CNN–LSTM)	Not used in the real agricultural environment
Padhy et al. (2023)	DoS attack	Integrates blockchain technology, fog computing, and software-defined networking	Insertion of fake Sensor data in the intelligent agricultural field
Negera et al. (2023)	Botnet attack	The lightweight deep learning model for an SDN-enabled IoT framework	Interpretability limitations: Incomplete feature identification
Alyahya et al. (2022)	Replay attacks, DoS attacks	Cyber Secured Framework for IoT devices using Constrained Application Protocol (CoAP)	Only tested in the simulated environment

4.6 Industrial IoT

IoT nowadays is being used in almost every field but it contributes widely to IIoT where smart factories and intelligent manufacturing take place (Sadeghi et al., 2015). As the security of IIoT is a major concern Wang et al. (2020) proposed a security technology for Industry 4.0. Blockchain is considered a relevant solution to the security of industrial IoT.

IIoT systems face significant security threats as depicted in Table 7, including false data injection attacks that manipulate sensor readings, routing attacks, DoS, botnet attacks, eavesdropping, and man-in-middle-attacks (Javed et al., 2022). Robust security measures such as AEs (Aboelwafa et al., 2020), deep learning methods (Yavuz et al., 2018), clustering models (Jing and Wang, 2022), and ECC (Yang et al., 2023) are crucial to protect IIoT environments.

4.7 Smart agriculture

IoT in agriculture is gaining popularity among countries that export agri products. Ferrag et al. (2020) classified five types of attacks including authentication, privacy, confidentiality, availability, and integrity to IoT-based agriculture. A 4-tier architecture of green IoT-based agriculture has been presented. It has also been described how blockchain-based public key infrastructure, machine learning, distributed key management, and access control solutions for security can be applied to IoT-based agriculture.

IoT security attacks, such as DoS and botnet attacks as described in Table 8, pose risks to smart agriculture. DoS attacks disrupt device availability, while botnet attacks use compromised devices for coordinated disruptions. These attacks can compromise farming processes, disrupt data collection, and compromise system integrity (Vangala et al., 2022). Neural network-based systems (Aldhyani and Alkahtani, 2023), blockchain technology with fog computing (Padhy et al., 2023), and deep learning models (Negera et al., 2023) can be used to protect smart agricultural systems.

5 IoT layers

As different applications use different IoT devices which are of varied nature in terms of performance, interaction, and data handling. Different devices are prone to unique threats that require customized security. Therefore, layered security provides the flexibility to adjust security measures in response to evolving threats. The IoT architecture is divided into 4 main layers where data flows from connected objects using sensors/actuators to gateways for digitization and protocol conversion, then to edge devices for pre-processing, and then finally to the cloud for detailed processing and storage. The processed information is then passed to the real world for use (Raj and Shetty, 2022). The layers of a core IoT application are shown in Figure 9.

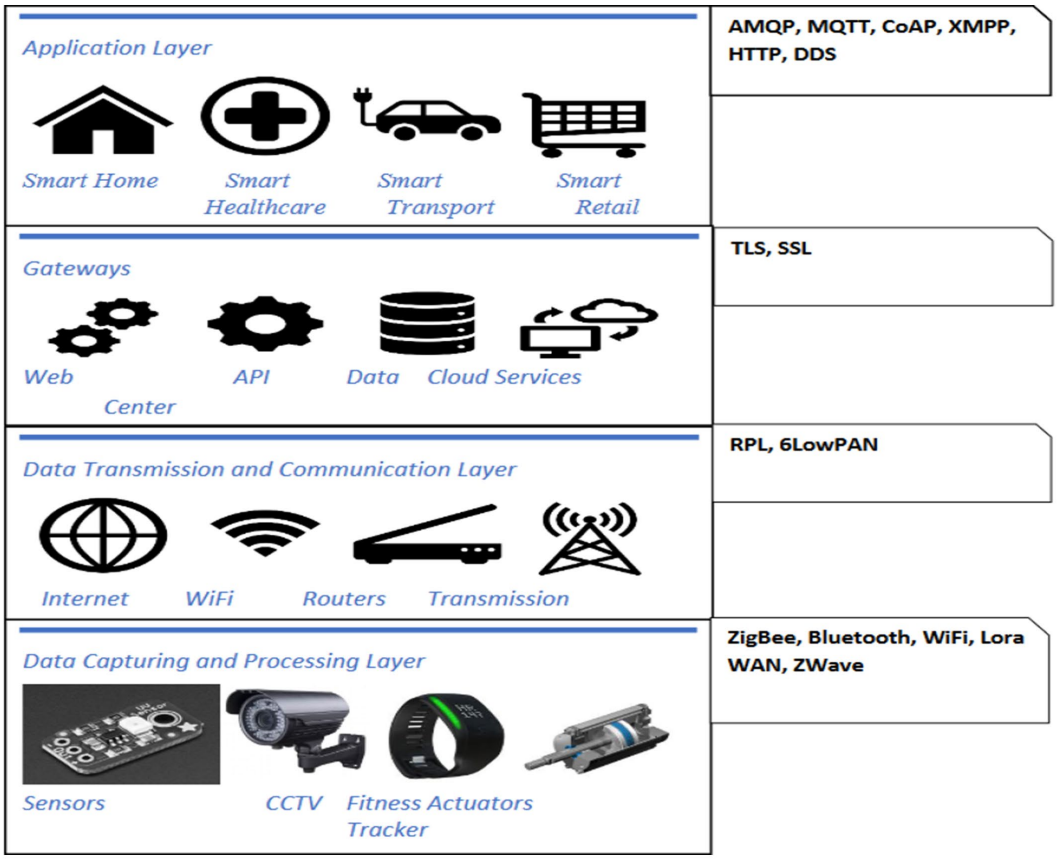

FIGURE 9
Layers of a core IoT application.

5.1 Data capturing and processing layer

In this layer, data is collected from the outer world with the help of sensors. A sensor can identify changes in a situation. Sensors are linked to IoT networks. Sensors collect data and then transform it into an electric signal. An actuator is a component of a machine that converts this electric energy to non-electrical energy such as motion (Rayes and Salam, 2022).

As sensors can be analog or digital, passive or active, or can be property-based (mechanical, chemical, etc.; Sehrawat and Gill, 2019). IoT connectivity protocols are used to connect devices over the network, allowing device-to-device communication within the range of the network (Al-Sarawi et al., 2017). IoT connectivity protocols are mainly defined on the Physical Layer that is discussed in Table 9:

(1) Zigbee: Zigbee is a protocol based on communication that follows the IEEE 802.15.4 standard. The main characteristics of ZigBee are low throughput, less energy consumption, and 100-meter connectivity between devices (Bhoyar et al., 2019). Smart homes, smart alarm systems, and surveillance systems are some of the applications where ZigBee is most used.

The most popular use of ZigBee is wireless sensor networks using mesh topology. Because of its self-configuration property, the installation and maintenance of ZigBee is effortless. Hundreds and thousands of nodes can easily be added to the ZigBee network and many devices such as sensors, microcontrollers, etc. are available in the market now using this open standard (Al-Sarawi et al., 2017).

(2) Bluetooth: Bluetooth is another open standard used for communication in the short range that allows wireless connections to a variety of electronic devices such as telephones, keyboards, computers, laptops, mice, palmtops, printers, headsets, speakerphones, and more. It is based on the IEEE 802.15.1 standard and its technical specifications include three categories with a range of 100, 10, and 1 meter (Bhoyar et al., 2019). The second most common category Is (10 m or 30 feet), which enables devices to be connected even on different floors (Lonzetta et al., 2018).

(3) Wi-fi: Wi-fi is used to connect to nearby devices that fall in a specific range. for broadcasting any data, various devices like computers/laptops/desktops or mobiles can use an internet connection which can be connected with wires or without wires. Radio waves are used by Wi-fi for broadcasting at 2.4 GHz and 5GHz frequencies. These frequencies have multiple paths which help many wireless devices to perform certain operations (Bhoyar et al., 2019).

5.2 Connectivity layer

Once the sensors collect the data, the next step is to convert it into a computer-readable format. As the data from the sensors comes in an analog form, for processing it needs to be converted into digital format. Data acquisition systems (DAS) are used to perform data aggregation

TABLE 9 IoT connectivity protocols.

Protocols	Layers	Bandwidth	Connectivity	Functions	Application area
ZigBee	Physical and MAC layer	Up to 250 Kbps	Many to many	Power consumption is less Low throughput Addressing Message exchange	Wireless sensor networks Personal area network (PAN) Smart Homes Smart Alarms Surveillance systems (Chen and Jin, 2012)
Bluetooth	Physical and Data Link Layer	24 Mbps	One-to-one	Low bandwidth Short-range connection	Smart phones Smart speakers (Collotta et al., 2018)
Wi-Fi	Physical Layer	54 Mbps	One-to-many	High data throughput High power consumption	Home security system Smart Grid (Li et al., 2011)
Zwave	Application Layer	100 Kbps	One-to-one	Interoperability Easy installation. Low power consumption Low interference. Security Scalability Open source Low cost	IoT home applications (Li et al., 2011)
Lora Wan	Media Access Control (MAC)	300 bps to 37.5 kbps	Many to many	Lora modulation technique Low power consumption Long range communication Bi-directional communication	Smart cities Smart metering (Tukade and Banakar, 2018)

TABLE 10 IoT connectivity layer protocols.

Protocols	Layers	Bandwidth	Connectivity	Functions	Application Area
6LowPAN	Networking technology or adaption layer	Up to 250 Kbps	One-to-many and many-to-one	Open Standard protocol Provides IP Addresses of Nodes Flexible and Self-Healing Mesh Routing	Automation Industrial monitoring Smart Grid Smart Home(Al-Sarawi et al., 2017)
RPL	Network layer	-	MultiPoint-to-Point (MP2P); Point-to-Point (P2P); Point-to-MultiPoint (P2MP).	Loop avoidance and detection Self-configuration	IoT network layer(Institute of Electrical and Electronics Engineers and IEEE Internet of Things (Initiative), 2020)

and convert the aggregation results into digital numeric values so that the Internet gateway can receive the digitized data and transmit it over the Internet for further processing (Jabraeil Jamali et al., 2020; Chatterjee and Ray, 2022). The main task of this layer is to choose the optimal routing path from one node to another in the network. The IoT connectivity layer protocols defined in Table 10 are described below:

(1) 6LOWPAN: 6LOWPAN Stands for Low power wireless personal area network over ipv6. information can be transmitted seamlessly even from devices that use low-speed processors using this protocol. It enables IEEE 802.15.4 radios To carry 128-Bit addresses of ipv6 (Sharma et al., 2018).
(2) Routing protocol(RPL): In the IoT connectivity layer, routing information is provided by the RPL, which Is an ipv6-based protocol. It is a standard protocol mainly used for resource-constrained devices over lossy links. The RPL protocol is based on a destination oriented directed acyclic graph(DODAG), which Is a directed acyclic graph that has one and only one root. This graph Is considered better than a tree as it allows nodes to have information about their parent nodes and allows them to select multiple neighboring nodes as parent nodes but they do not contain any information about child nodes. The major external attacks on RPL networks are confidentiality, integrity, and availability of services (Institute of Electrical and Electronics Engineers and IEEE Internet of Things (Initiative), 2020).

5.3 Gateways

The main function of gateways is protocol conversion. The gateways wrap and format the digitized data by the network protocol and after wrapping, data is stored in the cloud via the network. The

gateways are used: when different protocols are used by node and network and the other is when two devices need to communicate but using different protocols (Hassija et al., 2019). The IoT gateway protocols are discussed below:

(1) Secure socket layer (SSL): SSL Is used to exchange encrypted data to provide security so hackers are not able to access the data. To block cyber-attacks during transit, IoT SSL certificates Are used that encrypt the data using symmetric encryption between the IoT device and the application. The SSL certificate provides an extra layer of protection to user data through user authentication (Yugha and Chithra, 2020).
(2) Transport layer security (TLS): TLS is an improved and secure version of SSL. TLS is used in IoT to make connections secure between devices and remote servers. For TLS connection to work, some points need to be considered, such as mutual authentication between both parties, the use of symmetric encryption, and private keys. TLS uses a CA certificate that is signed by the certificate authority to validate the server. This certificate is then presented to the device by the server at the time of session establishment. TLS provides protection from cipher block chaining attacks and improved workstations and encryption models (Cynthia et al., 2019; Yugha and Chithra, 2020).

5.4 Application layer

The devices that use less power communicate by using Io data protocols. Direct communication is achieved using these types of protocols even with no internet connection as they use hardware that is placed on the user's side. Wired or wireless connectivity is possible through these protocols (Jabraeil Jamali et al., 2020). IoT data protocols are mainly defined on the Application Layer that is discussed in Table 11:

(1) Message Queue Telemetry Transport Protocol (MQTT): MQTT is an ISO standard lightweight protocol used with the TCP/IP suite. It is a publish/subscribe (pub/sub) messaging protocol. MQTT has three basic components: publishers, subscribers, and brokers. The publishers include different sensors that are used to collect data from various devices. The subscribers are those entities that use the sensor data and brokers act as a bridge between the publishers and subscribers, connecting them and classifying the sensor data (Yassein et al., 2018; Sidna et al., 2020).
(2) CoAP: it is an internet application protocol, particularly used for web transfer but used in a constrained environment with limited computational and communicational resources and bandwidth. CoAP is a client–server protocol like HTTP that uses UDP for lightweight implementation (Ugrenovic and Gardasevic, 2016).
(3) Advanced Message Queuing Protocol (AMQP): AQMP is an ISO open standard protocol that is used for queuing and routing messages with security and provides message delivery guarantees with three primitives at most once, at least once, and exactly once. The AQMP has three basic components, which are exchange, queue, and binding. The exchange component is used for receiving and routing messages to the queues. There are different separate queues for different processes and end customers use these queues to accept information. Bindings are the basic rules for distributing messages (Al-Fuqaha et al., 2015).

TABLE 11 IoT data protocols.

Protocols	Bandwidth	Connectivity	Functions	Application Area
MQTT	250 Kbps	One-to-one, one-to-many, and many-to-many	Minimum bandwidth use Low energy consumption Little processing and memory resources	Healthcare Logistics Industry and manufacturing Facebook Messenger for online chat Amazon Web services (Naik, 2017; Tukade and Banakar, 2018)
CoAP	40 Kbps	One-to-one and many-to-many communications	IoT systems that are based on HTTP protocol are handled here.	Machine-to-machine communication Smart energy (Yassein et al., 2018)
AMQP	250 Kbps	Point-to-point	Performing various functions such as collecting, arranging, and storing messages as well as their interrelationship.	Banking industry (Sidna et al., 2020)
HTTP	–	One-to-one	Building blocks for fetching web pages.	
DDS	64 Kbps	Peer-to-peer communication, one-to-one, one-to-many, many-to-many, and many-to-one	Installed in almost every device ranging from a minute to cloud based on real-time. Platform-independent data exchange is done.	M2M communications (al-Masri et al., 2020; Sidna et al., 2020)
XMPP	Upto 250 Kbps	One-to-one	Used in customer-based IoT applications due to features like flexibility skills.	Smart Grid Social Networking Consumer-oriented IoT applications (Al-Masri et al., 2020; Sidna et al., 2020)

(4) Hypertext Transfer Protocol (HTTP): Hypertext Transfer Protocol is the most common protocol of data communication for IoT devices over the web. HTTP is a stateless protocol for the communication of heterogeneous devices over the Internet. HTTP is a client–server-based protocol in which a client sends a request message and a host generates a response message. The basic flaws which have been encountered in HTTP are cost, battery life, and energy saving. But still, a large set of data is published by this (Naik, 2017; Sidna et al., 2020).
(5) Data Distribution Service (DDS): DDS is a protocol that deals in real-time and reliable performance which is deployed on platforms ranging from low-footprint devices and it uses multicasting to convey high quality. It is used as an IoT messaging protocol for communication between the sender and receiver (Naik, 2017).
(6) Extensible Messaging and Presence Protocol (XMPP): XMPP is a protocol used for exchanging messages in real time using a push mechanism. It is scalable and modifications can easily be accommodated. Open XML is used to develop this protocol so that the sender and receiver nodes' accessibility status can be provided. Some of the popular application areas of XMPP are gaming, which is online, news, WhatsApp, Google Talk, etc (Al-Masri et al., 2020).

6 IoT security threats LayerWise

The data is passed to various layers and nodes before reaching the user's device. As it crosses all nodes and different gateways, it is more vulnerable to attacks. IoT security attacks can occur at various layers of the IoT architecture, including the data capturing layer, data transmission layer, gateways, and application layer, compromising the overall security and integrity of IoT systems as shown in Figure 10.

6.1 Data capturing and processing

Changes in a situation can be identified by a sensor. Sensors are linked to IoT networks. Sensors collect data and then transform it into an electric signal. An actuator is a component of a machine that converts this electric energy to non-electrical energy such as motion (International Systems Engineering Symposium, 2015). Sensors detect electrical or optical signals and then transform these.

signals into electrical signals. A variety of sensors are available in the market for different purposes. Sensors can be monitored on various parameters like accuracy, precision, environment, etc. The major attacks that can be experienced at this stage are as follows:

(1) Node Capturing: In IoT applications, many sensors and actuators are used which are considered nodes with little consumption of power. These low-power devices are highly prone to security attacks by hackers in various activities. These low-power devices are highly prone to security attacks by hackers in various activities such as replacing or capturing the node with a malignant node (Sudeendra Kumar et al., 2018).
(2) Malicious Code Injection Attack: These types of attacks occur when some harmful code is inserted into the node's memory by the opponent. Firmware or software on IoT nodes is commonly updated over the air, giving attackers a gateway to insert malignant code. With this malignant code, it provides a loophole for suspicious users, so that they can have complete control of the system which is based on IoT, and perform actions according to them (Deogirikar and Vidhate, 2017).
(3) False Data Injection Attack: Once a node is created, an attacker can use it to insert incorrect data into the IoT system. This can lead to incorrect results and can cause IoT applications to crash. An attacker could also use this technique to commit a DDoS attack (Deogirikar and Vidhate, 2017).
(4) Side-Channel Attacks (SCA): Besides direct attacks on nodes, the leakage of sensitive data can cause multiple side-channel

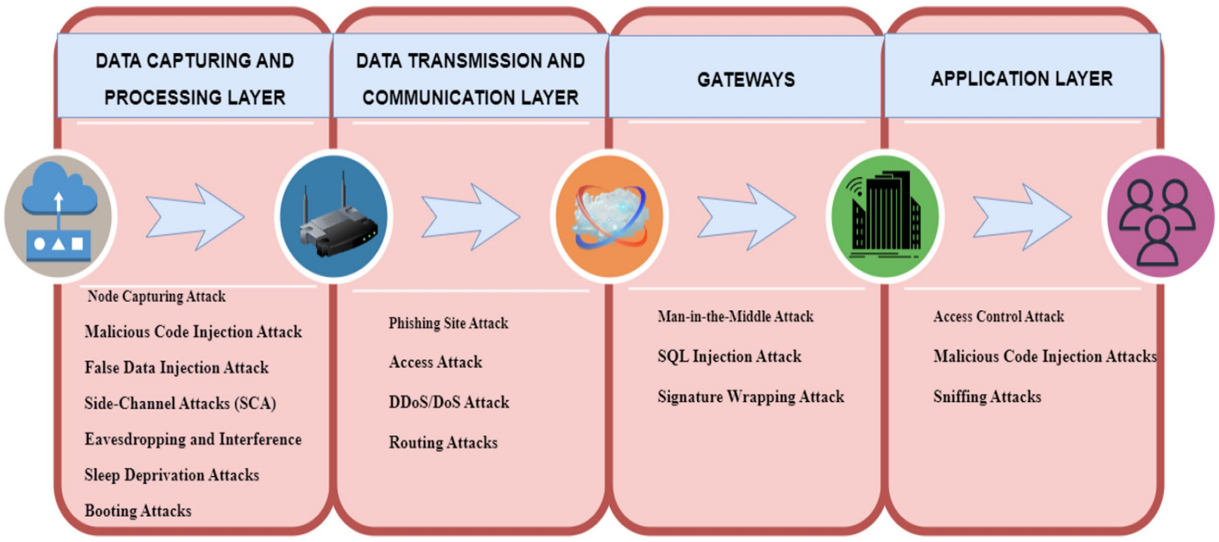

FIGURE 10
IoT layers unveiled: the battleground of security breaches.

attacks. Processor microarchitectures, electromagnetic radiation, and their power consumption provide opponents with sensitive information. Power consumption side-channel attacks, laser attacks, time attacks, or electromagnetic attacks are also supported. Modern chips provide several remedies to forestall these types of attacks when running cryptographic modules (Sayakkara et al., 2019).

(5) Eavesdropping and Interference: In an IoT open environment, usually different nodes are located to communicate between different IoT devices. This results in IoT applications being vulnerable to attacks during data transmission or authentication, data can be listened to and accessed (Liao et al., 2018).

(6) Sleep Deprivation Attacks: In these types of attacks, opponents tried to discharge the batteries of the IoT-Edge device with low power. Due to low battery, denial of service attacks on nodes for IoT applications occur. It can be achieved in two ways, which is one by performing endless loops on peripheral devices and by pretending the enhanced power consumption of peripherals using malicious code (Kamble and Bhutad, 2018).

(7) Booting Attacks: At the time of booting, inbuilt security techniques are disabled, so edge devices are more at risk of attacks during that time. Attackers could exploit the vulnerability and attempt to attack when the node devices restart. Because peripheral devices typically have low power consumption and sometimes go through a sleep-and-wake cycle, it is important to provide a secure boot process on those devices (Deogirikar and Vidhate, 2017).

6.2 Data transmission and communication

The prime responsibility of this layer is to transmit the information received from the data capturing and processing stage to the analytical unit for further processing. The considerable security attacks that can be experienced at this stage are as follows:

(1) Phishing Site Attack: These types of attacks happen when various IoT devices are attacked by hackers simultaneously and they anticipate that some devices will be compromised. Visitors who visit websites on the Internet are more likely to encounter phishing sites. After hacking the user credentials, attackers can cause harm to the entire IoT environment (De La Torre Parra et al., 2020).

(2) Access Attack: Another name for an access attack is Advanced Persistent Threat (APT). In such attacks, the IoT network is accessed by an attacker or opponent and stays there for an extended period. These types of attacks are not for destroying the network, rather they capture important information of users by unauthorized access. As crucial data of users is being transmitted in the IoT network, users' private information can be leaked (Liu et al., 2012).

(3) DDOS/DOS Attack: DDoS attacks occur when the hacker overloads the servers with more requests than a server could handle. This service to the end user has been disrupted as the server is disabled. When the server is filled with multiple resources by the hacker, a DDoS attack is likely to happen. These types of attacks are not IoT application specific, but the network layer of IoT is susceptible to these attacks due to the complexity and diversity of IoT networks. As IoT devices are not properly arranged, it enables hackers to launch DDoS attacks easily. The Mirai botnet attack exploited this susceptibility and as a result, many servers were being blocked by continuously sending requests to IoT servers (Kolias et al., 2017).

(4) Routing Attacks: Routing attacks occur during the data transmission phase where harmful nodes attempt to divert routing paths. There is a special type of attack known as a sinkhole attack where attackers grab the attention of nodes by showing a false shortest route and enabling the nodes to use that route only. Another type of routing attack is a warm-hole attack that could cause serious security issues if it is joined with a sinkhole attack as hackers try to avoid security protocols by using the combined attack (Yavuz et al., 2018).

6.3 Gateways

It is the stage where data is analyzed, managed, and stored on strong IT systems. More in-depth analysis can be done in this stage as sensor data is combined with data from other sources for deeper insights. This layer creates an interface between the data transmission and the application layer. The major security threats encountered in this layer are described as follows:

(1) Man-In-The-Middle Attack: The Publish-Subscribe model is used by the MQTT protocol for data transmission and on the client side, MQTT Broker is being used efficiently. This enables publishers and subscribers to communicate with each other and messages can be sent without destination information. After turning into a man-in-middle by controlling the broker, the full authority of communication can be held by the attacker without even informing the client (Tewari and Gupta, 2020).

(2) SQL Injection Attack: The gateways are vulnerable to SQL injection attacks. For such attacks, dangerous SQL statements are inserted by the hacker in a program (Kasim, 2021). In addition, hackers can retrieve any user's personal data and database tuples can be changed. SQL injection is a major security issue as listed in the Open Web Application Security Project (OWASP).

(3) Signature Wrapping Attack: At gateways, XML signatures are used for internet services. For this type of attack, the hacker can break the signature algorithm and perform the operation or manipulate the data by making use of susceptibilities (Hassija et al., 2019).

6.4 Application layer

The application layer creates a link between the user and the IoT system. All IoT applications such as smart healthcare, smart buildings, smart transport, etc. reside in this stage. This stage has security issues that are specific to the privacy of the users' data and the applications

they are using. The extensive security concerns at this stage are discussed below:

(1) Access Control Attack: Access control means only authorized users should have access to IoT data so that data is restricted to legitimate users only. But if that access is compromised, the whole IoT system will be at risk (Liu et al., 2012).
(2) Malicious Code Injection Attacks: The attacker injects malicious code or script from an unknown location into the system, hacking authorized user data and manipulating or stealing important information about the user (Kasim, 2021).
(3) Sniffing Attacks: The network traffic can be monitored using sniffer applications by the attacker, which leads to the revealing of confidential user data (Kiran et al., 2020).

7 Existing security solutions LayerWise

The various security attacks and their effect on IoT systems and existing solutions are described in Table 12.

7.1 Data capturing and processing

The existing solutions for given security attacks on this layer are described below.

(1) Node Capturing: For sensor-capture attacks in medical IoT, an improvement has been made to the authentication.
(2) protocol proposed by Fotouhi *et al* (Fotouhi et al., 2020). The new version is lightweight and uses login and biometric authentication to make the system highly secure against node-capturing attacks by enhancing protocol authentication speed and minimizing its computational cost (Lee et al., 2022).
(3) Malicious Code Injection Attack: To prevent malicious code injection attacks, a hardware-based Secure Return Address Stack (SRAS) is implemented with limited modifications to the processor as well as the Operating system. To overcome buffer overflow attacks, a multilayer software and hardware approach is proposed that is static as well as dynamic defenses. For securing computing devices, this hardware-based solution can be combined with existing software solutions (Mosenia and Jha, 2017).
(4) False Data Injection (FDI) Attack: FDI attacks can mislead any data by inserting incorrect information such as wrong details of sensor movements. Yavuz et al. (2018) used AEs to detect FDI attacks instead of support vector machine-based methods. AEs have many advantages over earlier methods such as it is easier to train them as labeling is not required and different types of attacks such as hidden data correlation structures are easily learned by them. Therefore, they can detect any change in these complex structures by using AE-based algorithms. The data that is affected by FDI attacks can be recovered using a denoising autoencoder to the original state. This approach has reduced execution time as well as a tendency for false alarms (Yavuz et al., 2018).
(5) SCA: For detecting side channel attacks in IoT networks, a packet obfuscation scheme is proposed using local differentiation privacy in smart home applications. Smart home devices such as cameras, switches, and sleep monitors are used to collect IoT data, and privacy bandwidth trade-offs have been shown with consideration of some assumptions (IEEE Signal Processing Society, 2018).
(6) Eavesdropping: Initially, eavesdropping in IoT was solved with the use of encryption and decryption methods, but due to constrained resources in IoT, it is difficult to implement.
(7) Xu et al. (2016) have given relay transmission as a solution to eavesdropping. As several hurdles in information transmission come from machinery/equipment noise and vibrations, it is necessary to deploy relaying in most IoT environments.
(8) Sleep Deprivation Attacks: The main aim of this attack is to degrade the battery life of target nodes by utilizing their power consumption to the full extent. Bhattasali and Chaki (Bhattasali and Chaki, 2011) suggest a lightweight multilayer IDS without using MAC protocols. This multilayer technique uses the cluster-based approach for plotting IDS.
(9) Booting Attacks: To protect from booting attacks, hardware-based security implementation is essential. For this, a FPGA is used to protect infrastructural components. An IoT device is being designed using a ZC-706 prototype board which is the master of the booting process. To secure the IoT device, three things have been done. First, an IoT device is protected from bit stream encoding by encrypting the FPGA bit stream. Second, the system boot image is encrypted and lastly, it has been checked that FPGA is working correctly so that attacks like spoofing and Trojan horses can be avoided (Tufts University and IEEE Circuits and Systems Society, 2017).

7.2 Data transmission and communication

The existing solutions for given security attacks on this layer are described below:

(1) Phishing Site Attack: Phishing attacks deal with the user's financial information such as hacking passwords, so that IoT devices can be hacked. Dhillon and Kalra (2017) introduced Phish-sec mathematically by using interactive intersection to find out website uniqueness. The Phish-sec is considered efficient as it evades data poisoning to secure the back-end system.

To detect counterfeited web pages, machine learning algorithms such as artificial neural networks, decision trees, support vector machines, etc. are used but proper features need to be selected for classification. Therefore Sabahno and Safara (2021) suggested an ISHO algorithm that is based on a hyena optimization algorithm with swarm hunting of spotted hyenas. The major developments in this algorithm are local as well as global search and are improved, being converted into binary, and a support vector machine is combined with a feature selection method so that phishing can be detected. The proposed algorithm has proved to be efficient in comparison to other meta-heuristic algorithms.

TABLE 12 IoT security attacks and solutions.

Layers	Type of security attack	Effect on IoT system	Existing solutions
Data capturing and processing	Node capturing	The original node was replaced with the malicious node	Improvement in the authentication protocol (Chen et al., 2021)
	Malicious Code Injection Attack	Attack on node's memory	Secure Return Address Stack (SRAS) (Lee et al., 2022)
	False Data Injection Attack	Insertion of incorrect data	AEs (Aboelwafa et al., 2020)
	SCA	Leakage of secret keys	Packet obfuscation scheme (IEEE Signal Processing Society, 2018) Robust Encryption Algorithm (Fernández-Caramés and Fraga-Lamas, 2018) De patterning and decentralization (Mosenia and Jha, 2017)
	Eavesdropping and interference	Data leakage	Relay transmission (Xu et al., 2016) Chaos based cryptography (Song et al., 2017)
	Sleep deprivation attacks	Draining the batteries of edge devices	Lightweight multilayer IDS (Bhattasali and Chaki, 2011)
	Booting attacks	Sensitive sections of hardware and software are at risk.	Field Programmable Gate Array (Tufts University and IEEE Circuits and Systems Society, 2017)
Data transmission and communication	Phishing site attack	Multiple IoT devices can be attacked	Phish-sec using interactive intersection(Nirmal et al., 2020) ISHO algorithm (Sabahno and Safara, 2021) Distributed deep learning framework (De La Torre Parra et al., 2020)
	Access attack	Unauthorized access	Role-based access scheme (Liu et al., 2012) Three-factor remote user authentication scheme (Dhillon and Kalra, 2017) Ultra-weight RFID authentication protocol (Safkhani and Bagheri, 2017) New signature-based authentication key establishment scheme (Chifor et al., 2018)
	DDoS/Dos attack	Blocked server due to many attacks	IDS framework (Kasinathan et al., 2013) Packet marking, filtering, and dropping mechanisms(Zargar et al., 2013)
	Routing attacks	Routing paths are disrupted, and a DoS attack can be launched	IDS using Clustering and Reliability modules (Santos et al., 2019) Deep learning on Big Data(Yavuz et al., 2018) Hashing and Signature-based authentication (Dvir et al., 2011) Monitoring node behavior (Le et al., 2013)
Gateways	Man-in-the-middle attack	Communication control	Locality sensitive hashing(LSH) (Salem et al., 2022) IDS and IPS in fog nodes (Aliyu et al., 2018)
	SQL injection attack	Alteration of records in the database	Snort is a signature-based IDS (Gupta and Sen Sharma, 2022) TransSQL (Zhang et al., 2011) Ensemble classification algorithm (Kasim, 2021)
	Signature wrapping attack	Modifying messages in SOAP	Node counting (Gupta and Santhi Thilagam, 2016)
Application	Access control attack	Unauthorized user access	Certificate-based device-to-device access control (Chaudhry et al., 2021) Multi-factor authentication and session key agreement protocol (Amin et al., 2016) Lightweight authorization stack for untrusted cloud platform (Chifor et al., 2018) Authentication protocol using smart card(Amin et al., 2018) Certificate free authentication (Lavanya and Natarajan, 2017)
	Malicious code injection attacks	Hijacking of an IoT account	Status-based detection system (Wei and Qiu, 2018) Lightweight biometric authentication and key agreement (Dhillon and Kalra, 2017)
	Sniffing attacks	Access to confidential user data	Machine learning models (Kiran et al., 2020)

10.3389/fcomp.2024.1420680

A distributed deep learning framework is proposed for detecting phishing attacks which are cloud-based with two security algorithms, a Distributed CNN model within IoT devices as an add-on security feature to protect IoT devices from phishing attacks as soon as they occur and LSTM network mode to detect DDoS phishing attacks among various IoT devices. It has been shown that the proposed model can detect phishing attacks at the device level as well as at the back-end level (Liu et al., 2012).

(2) Access Attack: Role-based access schemes are used for access control. A role here means some particular function that can be one activity or group of activities that are associated with that function. No authorization is given to users, but they are assigned to roles. Roles control user access as well as their resources, which makes a hierarchy where roles come first and then corresponding users (Kasim, 2021).
(3) DDoS/DoS Attack: Santos et al. (2019) proposed an IDS framework for detecting DoS attacks in 6LoWPAN. The proposed system has two main components: one is a detection engine that is embedded in the framework itself and the other is a monitoring system. The performance of the proposed framework assessed by penetration testing has proved to be more stable. Suricata (IDS), Prelude (SIEM), and SCapy (PenTest), like open-source security tools, are used for development.
(4) Routing Attacks: Kesswani and Agarwal (2020) suggested an IDS using Clustering and Reliability modules, that is used for preventing sinkhole and selective forwarding attacks on routing mechanisms in IoT networks. By simulation, it has been shown that routing attacks can be detected, and the efficiency of the proposed approach is also shown.

Routing attacks in IoT can be detected by using deep learning on Big Data. IoT routing attacks that are hello flood, decrease rank and version number modification attacks can be detected using the Cooja IoT simulator with Cotinki-RPL implementation. The proposed model is well-suited for real-life IoT applications with high precision and recall rates (Jing and Wang, 2022).

7.3 Gateways

The existing solutions for various security attacks on this layer are described below:

(1) Man-In-The-Middle Attack: To prevent man-in-middle attacks and fake alarms, a framework is proposed by Salem et al. (2022) for use in the healthcare system. Three things are considered in the proposed system: privacy, reliability, and energy consumption of the healthcare system. LSH is used to drive digital signatures that are transmitted to get access to private data. A HMAC is sent to avoid modification attacks based on the Received Signal Strength Indication (RSSI) key. It has been shown that the proposed framework provides an accurate and low false alarm rate for attack detection. For preventing Man-in-Middle attacks in Fog Computing, IDS and IPS are proposed by Gupta and Sen Sharma (2022). Fog nodes are examined by IDS nodes one hop away and their content, context, and arrival time are recorded. IPS uses AES encryption techniques to avoid attacks.
(2) SQL Injection Attack: To detect SQL injection attacks and snort, a signature-based IDS is being used. Snort is an open-source IDS and can be used with all applications. To make the snort more effective and use it to detect all types of attacks, five new rules are proposed. The rules use white spaces, comments, hexadecimal equivalent values, strings, and semicolons. On the server side, Open WebGoat is being used to analyze the proposed system which is considered more effective (Zhang et al., 2011).

To solve the problems of SQL injection attacks, TransSQL is used which is a server-side solution that will automatically translate SQL queries to an LDAP request. TransSQL is used to analyze different responses from SQL and LDAP databases so that it can prevent SQL injection attacks (Gupta and Santhi Thilagam, 2016).

To protect against SQL injection attacks, a middleware application is developed using an ensemble classification algorithm. In this algorithm, SQL injections are divided into four main parts: clean, simple, unified, and lateral. In the case of simple injections, the SQL query is blocked. The IP address is blocked when lateral or unified injections occur. It has been shown that the developed method gives effective protection against SQL injection attacks (Chen et al., 2021).

(3) Signature Wrapping Attack: Making Simple Object Access Protocol (SOAP) messages secure means web services are being protected from attackers. SOAP messages use digital signatures to protect the data. But that can be modified by the attackers without invalidating the signature. Therefore Amin et al. (2016) have proposed a solution to a signature wrapping attack by using node counting. In a web service request, the frequency of each node is calculated to detect wrapping attacks. It has been shown that the proposed solution is much more effective in detecting such attacks.

7.4 Application layer

The existing solutions for given security attacks on this layer are described below:

(1) Access Control Attack: To protect from access control attacks in healthcare, ECC is used to propose certificate-based device-to-device access control which ensures the safety of all other devices if any device is compromised. Although this proposed model has additional computational, and other costs it can protect the system from unauthorized or man-in-middle-attacks (Chaudhry et al., 2021).
(2) Malicious Code Injection Attacks: Wei and Qiu (2018) suggested a status-based detection system that will detect any malicious task done by IoT devices by continuously checking the running status of the device. The infected IoT device can easily be detected by checking its activities like monitoring the operations of the web camera. Any change in device activity is identified using simulation.
(3) Sniffing Attacks: Machine learning models are being used by Kiran et al. (2020) to detect sniffing attacks. To classify the data

as normal and attack data, four machine learning algorithms: Support Vector Machine (SVM), Naïve Bayes, Decision Tree, and Adaboost are being used to test the simulated IoT environment by using NodeMCU. The data transmission is done between NodeMCU and the ThingSpeak Server. An IDS is designed to overcome sniffing attacks.

8 Discussion

IoT security attacks pose significant challenges and prompt discussions regarding the vulnerabilities and potential consequences they bring to various applications. One of the primary concerns is the increasing number of IoT devices being deployed without adequate security measures. This lack of security leaves devices susceptible to attacks, leading to potential privacy breaches, data theft, and even physical harm (Ullah et al., 2024). One of the prominent security attack vectors is the DDoS attacks (Kasinathan et al., 2013). By compromising numerous IoT devices and coordinating them to flood a target system or network with an overwhelming amount of traffic, attackers can disrupt operations, rendering critical services unavailable. These attacks exploit weak security configurations and vulnerabilities present in many IoT devices (Bala and Behal, 2024; Reegu et al., 2024; Singh and Jain, 2024).

Another type of attack is device spoofing or impersonation, where attackers mimic legitimate IoT devices to gain unauthorized access to networks or systems (Kesswani and Agarwal, 2020). This can lead to unauthorized control, data manipulation, or the infiltration of sensitive information. Insecure communication channels, weak authentication mechanisms, and lack of secure firmware updates are often the entry points for such attacks (Ghaffari et al., 2024). Additionally, IoT devices often collect and transmit sensitive data, raising concerns about data privacy and integrity. Attackers may intercept, manipulate, or steal this data, posing a significant risk to individuals and organizations. Furthermore, the compromised devices themselves can become platforms for launching further attacks, creating a ripple effect across interconnected systems (Negera et al., 2023; Toman et al., 2024).

The complexity of IoT systems, with numerous interconnected devices, poses another challenge. Discussions revolve around securing the entire ecosystem, including gateways, communication channels, cloud infrastructure, and end devices (Tewari and Gupta, 2020). Implementing secure protocols (Yugha and Chithra, 2020; Khilar et al., 2022), encryption algorithms (Dhar Dwivedi and Srivastava, 2022; Liu et al., 2022), and access control mechanisms (Chaudhry et al., 2021; Farhad Aghili et al., 2022) is critical to protecting sensitive data and ensuring secure communication among devices. The study of IoT Security Attack Types, Application Areas, Challenges, and Mitigation Strategies as discussed in Table 13 is a vital exploration that encompasses the multifaceted landscape of IoT security. By analyzing different attack types such as botnet attacks (Singh et al., 2024) that are used to compromise numerous connected systems, spoofing (Reddy et al., 2024; Xu et al., 2024) which is an act of deceiving, and man-in-the-middle attacks (Bin Muzammil et al., 2024; Thankappan et al., 2024) that alters the communication between two parties, researchers gain insights into the vulnerabilities and risks faced by IoT systems. Understanding the application areas impacted by these attacks, including smart homes, industrial automation, and healthcare, highlights the potential consequences and the need for robust security measures.

To address these challenges, discussions revolve around implementing robust security measures at multiple layers. The development of industry-wide security standards and best practices is also a topic of discussion, promoting uniform security guidelines for IoT device manufacturers and application developers.

Furthermore, discussions focus on the role of artificial intelligence (Chen et al., 2021) and machine learning (Ahmad and Alsmadi, 2021; Sarker et al., 2023; Ni and Li, 2024) in IoT security. These technologies can help detect anomalies, identify potential threats, and enhance incident response capabilities. Deploying intelligent security systems that can adapt to emerging attack patterns and quickly respond to threats is a key area of exploration (Inuwa and Das, 2024).

Researchers propose solutions to mitigate IoT security attacks, but they come with limitations. Secure communication protocols, such as TLS or IPsec, provide robust security but may be challenging for resource-constrained IoT devices (Mohanty et al., 2020). Segmentation and network isolation can contain breaches but may introduce complexity and impact scalability. AI and machine learning can detect anomalies, but distinguishing between legitimate and malicious activities can be difficult. Practical solutions should address evolving threats in the dynamic IoT landscape. Most of the solutions given by researchers work in simulated environments, so a lot of work is required to implement them in real-world environments (Fotouhi et al., 2020; Aldhyani and Alkahtani, 2023; Ali et al., 2023). Overcoming limitations and barriers is necessary to develop effective IoT security solutions.

Overall, the discussions surrounding IoT security attacks emphasize the need for a multi-faceted approach that encompasses robust device security, regular updates, secure communication protocols, continuous monitoring, and collaborative efforts. By addressing these challenges head-on, the IoT community can strengthen the security posture of IoT applications and build a more resilient and trustworthy ecosystem.

9 Conclusion and future scope

IoT is not a single technology but it is a combination of diverse technologies, such as cloud computing, fog computing, edge computing, machine learning technologies, and many more. It has been wrapped up that various devices such as sensors, actuators, and RFID are used in core IoT applications to provide intelligent services to users. The various messaging and networking protocols are used to support the IoT deployment process. It has been concluded that the crucial IoT data is being processed to various IoT access points for further processing before reaching the end device, so the data should be secured from various routing, booting, injection attacks, and unauthorized access. In this paper, protocols used in different layers and related security issues are presented. The existing mitigation strategies to IoT security challenges including machine learning, Blockchain, IDS, and encryption algorithms are unveiled. Undoubtedly, IoT security has become a major problem; nevertheless, as per the discussion in Table 13, it is evident, that there is still a

TABLE 13 IoT security attack types, application areas, challenges, and mitigation strategies.

Security attack	Core IoT application	Challenges	Mitigation strategies
DoS attack	Smart Healthcare Smart City Smart Home Cloud Computing Industrial IoT Smart Agriculture	Blocked server due to many attacks	Deep neural network-based cyber-attack detection system (Vijayakumar et al., 2023) Attack detection model (Velliangiri et al., 2023) IDS framework (Kasinathan et al., 2013) WFL (Ali et al., 2023) PCA-FCM clustering model (Jing and Wang, 2022) CNN–LSTM (Aldhyani and Alkahtani, 2023)
Spoofing	Smart Home Smart Healthcare	Preventing deceptive impersonation and manipulation	RFID-enabled multifactor authentication model (Kesswani and Agarwal, 2020) Neural network-based cyber-attack detection system (Vijayakumar et al., 2023)
Man-in-middle attack	Smart Healthcare Cloud Computing Industrial IoT	Communication control	Framework using LSH and HMAC (Salem et al., 2022) Regression modeling (Sivasankari and Kamalakkannan, 2022) ECC and trusted tokens with packet encryption using the TLS protocol (Yang et al., 2023)
Access control attack	Smart healthcare smart home	Unauthorized user access	ECC (Chaudhry et al., 2021) Context-aware security-based scheme (Khanpara et al., 2023)
Botnet attacks	Industrial IoT smart agriculture	Mitigating distributed threats with coordinated defense	Real-time network environment (Kumar Donta et al., 2023) The lightweight deep learning model for an SDN-enabled IoT framework (Negera et al., 2023)

substantial gap in the amount of work devoted to resolving this issue. It has been determined that IoT is certainly becoming more and more essential, but research and development efforts have not kept pace with the need to strengthen its security. This discrepancy highlights the pressing need for a more substantial commitment to IoT security research and implementation to match the growing significance of IoT technology. This survey is anticipated as a valuable source of IoT security intensification for forthcoming applications. For researchers and readers, this review also provides useful perspectives to improve IoT security.

This survey provides valuable insights and guidance for young researchers, directing their focus toward the crucial realm of IoT data security. Exploring the challenges and mitigation strategies aims to raise awareness and foster a deeper understanding of this critical field. Through comprehensive analysis and recommendations, it empowers young researchers to contribute toward securing IoT environments and safeguarding sensitive data. With its emphasis on healthy direction, this survey paves the way for impactful research in the realm of IoT data security.

- AES and DES cryptography techniques are being widely used to encrypt the data whereas the ECC algorithm can be used to recover from side-channel attacks, but still no work has been done using ECC. In comparison to other algorithms, the ECC algorithm is smaller in size, which makes it suitable for mobile devices (IEEE Signal Processing Society, 2018).
- In the future, another swarm meta-heuristic algorithm can be examined. There are a lot of growing and successful meta-heuristic algorithms such as gray wolf and glow worm optimization algorithms available in swarm intelligence that could be investigated. A real dataset can be used in the proposed approach in the future so that phishing attacks can be avoided (Sabahno and Safara, 2021).
- New machine learning techniques can be discovered with reduced communication overhead and computation. To make IoT devices more secure and reliable, machine learning-based backup recovery mechanisms should be designed (Xiao et al., 2018). Deep learning provides solutions in the case of IDS but requires more time to train the model, sometimes a week or even a month. For attack detection, both stateless and stateful traffic feature analysis is required but models are trained for one approach only. ML and DL datasets should be trained on IoT-specific data (Ahmad and Alsmadi, 2021).
- The algorithm and training model can be separated and stored in the cloud in the future so that data from gateways can easily be organized and examined and then decide which machine learning detection algorithm can be applied (Wei and Qiu, 2018).
- A lightweight security protocol should be designed because of resource-constrained IoT devices. System throughput and consensus algorithm problems are still there because IoT devices are connected in huge numbers (Mohanta et al., 2020). There should be some security protocols for handling large IoT data effectively (Mohanty et al., 2021). In the future, a standard protocol will be required to fulfill the security needs of heterogeneous IoT devices (Yugha and Chithra, 2020).
- Till now, IoT is related to technology only. However, it should be applied to other areas such as management, economics, sociology, law, etc (Tewari and Gupta, 2020). The work can be expanded in the future so that upcoming attacks in IoT communication such as using encrypted data to avoid detection (De La Torre Parra et al., 2020).

- There is a need to reduce the energy spent by the blockchain model and it also should be deployed to other application areas than smart homes (Mohanty et al., 2020).
- To detect complex attacks, SNMP can be incorporated into Prelude (Kasinathan et al., 2013).
- The future idea is to develop a zero-trust IoT threat model to weaken various IoT security issues (Noor and Hassan, 2019; Dhiman et al., 2024).
- There is a need to verify ownership of data, that is how the data access will be controlled and a mechanism is required to assist deduplication of data (Yan et al., n.d.).
- SRAS can be applied to prevent DDoS attacks (Wani et al., 2021; Lee et al., 2022).
- In the future, the derived authentication key could be used in a pseudo-random function to detect jamming and channel hoping attacks (Salem et al., 2022).

Author contributions

KK: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Software, Validation, Writing – original draft, Writing – review & editing. AK: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Software, Validation, Writing – original draft, Writing – review & editing, Supervision. YG: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Software, Supervision, Validation, Writing – original draft, Writing – review & editing, Funding acquisition, Resources, Visualization. VG: Conceptualization, Data curation, Methodology, Validation, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This work was supported by the Deanship of Scientific Research, the Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (GRANTA099).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Aboelwafa, M. M. N., Seddik, K. G., Eldefrawy, M. H., Gadallah, Y., and Gidlund, M. (2020). A machine-learning-based technique for false data injection attacks detection in industrial IoT. *IEEE Internet Things J.* 7, 8462–8471. doi: 10.1109/JIOT.2020.2991693

Ahanger, T. A., Tariq, U., Ibrahim, A., Ullah, I., Bouteraa, Y., and Gebali, F. (2022). Securing IoT-empowered fog computing systems: machine learning perspective. *Mathvol* 10:1298. doi: 10.3390/MATH10081298

Ahemd, M. M., Shah, M. A., and Wahid, A. (2017). IoT security: a layered approach for attacks and defenses. *Int. Conf. Commun. Technol. ComTech* 2017, 104–110. doi: 10.1109/COMTECH.2017.8065757

Ahmad, R., and Alsmadi, I. (2021). *Machine learning approaches to IoT security: a systematic literature review[formula presented]*. Internet of things (Netherlands), No. 14. Elsevier B.V. p. 100365.

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., and Jalil, Z. (2022). Cyber security in IoT-based cloud computing: a comprehensive survey. *Electron* 11:16. doi: 10.3390/ELECTRONICS11010016

Aldhyani, T. H. H., and Alkahtani, H. (2023). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: deep learning model. *Math* 11:233. doi: 10.3390/MATH11010233

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tutorials* 17, 2347–2376. doi: 10.1109/COMST.2015.2444095

Ali, M. N., Imran, M., Ud Din, M. S., and Kim, B. S. (2023). Low rate DDoS detection using weighted federated learning in SDN control plane in IoT network. *Appl. Sci.* 13:1431. doi: 10.3390/APP13031431

Aliyu, F., Sheltami, T., and Shakshuki, E. M. (2018). A detection and prevention technique for man in the middle attack in fog computing. *Proc. Comput. Sci.* 141, 24–31. doi: 10.1016/j.procs.2018.10.125

Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., et al. (2020). Investigating messaging protocols for the internet of things (IoT). *IEEE Access* 8, 94880–94911. doi: 10.1109/ACCESS.2020.2993363

Al-Sarawi, S., Anbar, M., Alieyan, K., and Alzubaidi, M. (2017). *Internet of things (IoT) communication protocols: review*. 8th International Conference on Information Technology, pp. 685–690.

Alyahya, S., Khan, W. U., Ahmed, S., Marwat, S. N. K., and Habib, S. (2022). Cyber secure framework for smart agriculture: robust and tamper-resistant authentication scheme for IoT devices. *Electron* 11:963. doi: 10.3390/ELECTRONICS11060963

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., and Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Comput. Netw.* 101, 42–62. doi: 10.1016/J.COMNET.2016.01.006

Amin, R., Kumar, N., Biswas, G. P., Iqbal, R., and Chang, V. (2018). A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment. *Futur. Gener. Comput. Syst.* 78, 1005–1019. doi: 10.1016/J.FUTURE.2016.12.028

Aydos, M., Vural, Y., and Tekerek, A. (2019). Assessing risks and threats with layered approach to internet of things security. *Meas. Control* 52, 338–353. doi: 10.1177/0020294019837991

Bala, B., and Behal, S. (2024). AI techniques for IoT-based DDoS attack detection: taxonomies, comprehensive review and research challenges. *Comput Sci Rev* 52:100631. doi: 10.1016/j.cosrev.2024.100631

Ben Othman, S., Almalki, F. A., and Sakli, H. (2022). Internet of things in the healthcare applications: overview of security and privacy issues. *Intell. Healthc.* 2022, 195–213. doi: 10.1007/978-981-16-8150-9_9

Bhattasali, T., and Chaki, R. (2011). *A survey of recent intrusion detection systems for wireless sensor network*.

Bhoyar, P., Sahare, P., Dhok, S. B., and Deshmukh, R. B. (2019). Communication technologies and security challenges for internet of things: a comprehensive review. *AEU-Int. J. Electron. C.* 99, 81–99. doi: 10.1016/j.aeue.2018.11.031

Bin Muzammil, M., Bilal, M., Ajmal, S., Shongwe, S. C., and Ghadi, Y. Y. (2024). Unveiling vulnerabilities of web attacks considering man in the middle attack and session hijacking. *IEEE Access* 12, 6365–6375. doi: 10.1109/ACCESS.2024.3350444

Botnets Latest News, Photos and Videos WIRED. (2022). Available at: https://www.wired.com/tag/botnets/ (Accessed Aug 12, 2022).

Chatterjee, U., and Ray, S. (2022). Security issues on IoT communication and evolving solutions. *Stud. Comput. Intell.* 988, 183–204. doi: 10.1007/978-981-16-4713-0_10

Chaudhry, S. A., Irshad, A., Nebhen, J., Bashir, A. K., Moustafa, N., al-Otaibi, Y. D., et al. (2021). An anonymous device to device access control based on secure certificate

for internet of medical things systems: an anonymous D2D access control scheme for IoMT. *Sustain. Cities Soc.* 75:103322. doi: 10.1016/j.scs.2021.103322

Chen, X.-Y., and Jin, Z.-G. (2012). Research on key technology and applications for internet of things. *Phys. Procedia* 33, 561–566. doi: 10.1016/J.PHPRO.2012.05.104

Chen, C. M., Li, Z., Chaudhry, S. A., and Li, L. (2021). Attacks and solutions for a two-factor authentication protocol for wireless body area networks. *Secur. Commun. Netw.* 2021:593. doi: 10.1155/2021/3116593

Chen, J., Ramanathan, L., and Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocess. Microsyst.* 81:103722. doi: 10.1016/j.micpro.2020.103722

Chifor, B. C., Bica, I., Patriciu, V. V., and Pop, F. (2018). A security authorization scheme for smart home internet of things devices. *Futur. Gener. Comput. Syst.* 86, 740–749. doi: 10.1016/J.FUTURE.2017.05.048

Cho, Y., Oh, J., Kwon, D., Son, S., Lee, J., and Park, Y. (2022). *A secure and anonymous user authentication scheme for IoT-enabled smart home environments using PUF*.

Collotta, M., Pau, G., Talty, T., and Tonguz, O. K. (2018). Bluetooth 5: a concrete step forward toward the IoT. *IEEE Commun. Mag.* 56, 125–131. doi: 10.1109/MCOM.2018.1700053

Cynthia, J., Parveen Sultana, H., Saroja, M. N., and Senthil, J. (2019). Security protocols for IoT. Berlin: Springer International Publishing.

Inuwa, M. M., and Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. *Internet Things (Netherlands)* 26:101162. doi: 10.1016/j.iot.2024.101162

De La Torre Parra, G., Rad, P., Choo, K. K. R., and Beebe, N. (2020). Detecting internet of things attacks using distributed deep learning. *J. Netw. Comput. Appl.* 163:102662. doi: 10.1016/j.jnca.2020.102662

Deogirikar, J., and Vidhate, A. (2017). Security attacks in IoT: a survey. *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC* 2017, 32–37. doi: 10.1109/I-SMAC.2017.8058363

Dhar Dwivedi, A., and Srivastava, G. (2022). Open software and data security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK. *Internet Things* 2022:677. doi: 10.1016/j.iot.2022.100677

Dhillon, P. K., and Kalra, S. (2017). A lightweight biometrics based remote user authentication scheme for IoT services. *J. Inf. Secur. Appl.* 34, 255–270. doi: 10.1016/J.JISA.2017.01.003

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., et al. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors* 24:1328. doi: 10.3390/s24041328

Dvir, A., Holczer, T., and Buttyan, L. (2011). VeRA - version number and rank authentication in RPL. Proceeeding–8th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 709–714.

Farhad Aghili, S., Sedaghat, M., Singelée, D., and Gupta, M. (2022). MLS-ABAC: efficient multi-level security attribute-based access control scheme. *Futur. Gener. Comput. Syst.* 131, 75–90. doi: 10.1016/j.future.2022.01.003

Fernández-Caramés, T. M., and Fraga-Lamas, P. (2018). A review on the use of Blockchain for the internet of things. *IEEE Access* 6, 32979–33001. doi: 10.1109/ACCESS.2018.2842685

Ferrag, M. A., Shu, L., Yang, X., Derhab, A., and Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: review, Blockchain solutions, and challenges. *IEEE Access* 8, 32031–32053. doi: 10.1109/ACCESS.2020.2973178

Fontanella, F., Sakka, S., Liagkou, V., and Stylios, C. (2023). Exploiting security issues in human activity recognition systems (HARSs). *Inf.* 14:315. doi: 10.3390/INFO14060315

Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., and Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Comput. Netw.* 177:107333. doi: 10.1016/J.COMNET.2020.107333

Ghaffari, A., Jelodari, N., Pouralish, S., Derakhshanfard, N., and Arasteh, B. (2024). Securing internet of things using machine and deep learning methods: a survey. *Clust. Comput.* 1, 1–25. doi: 10.1007/s10586-024-04509-0

Gupta, A. N., and Santhi Thilagam, P. (2016). Detection of XML signature wrapping attack using node counting. *Smart Innov. Syst. Technol.* 49, 57–63. doi: 10.1007/978-3-319-30348-2_5

Gupta, A., and Sen Sharma, L. (2022). A novel approach for detecting SQL injection attacks using snort. *J. Inst. Eng. Ser. B* 103, 1443–1451. doi: 10.1007/s40031-022-00749-z

H1 Healthcare Data Breach Report. (2022) *Critical insight*. Available at: https://cybersecurity.criticalinsight.com/2021_healthcare_data_breach_report (Accessed June 25, 2022).

Hammi, B., Zeadally, S., Khatoun, R., and Nebhen, J. (2022). Survey on smart homes: vulnerabilities, risks, and countermeasures. *Comput. Secur.* 117:102677. doi: 10.1016/J.COSE.2022.102677

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access* 7, 82721–82743. doi: 10.1109/ACCESS.2019.2924045

IEEE Signal Processing Society (2018). IEEE international conference on acoustics, speech and signal processing: Proceedings: April 15–20, 2018. Calgary, Alberta, Canada: Calgary Telus Convention Center.

Institute of Electrical and Electronics Engineers and IEEE Internet of Things (Initiative). (2020). *IEEE world forum on internet of things, WF-IoT 2020 - symposium proceedings*. IEEE World Forum on Internet of Things, WF-IoT 2020 - Symposium Proceedings.

International Systems Engineering Symposium (2015). Internet of things (IoT): a literature review. *J. Comput. Commun.* 3, 164–173. doi: 10.4236/JCC.2015.35021

Internet of Things. (2022). *Key Business Insights Gartner*. Available at: https://www.gartner.com/en/information-technology/insights/internet-of-things (Accessed Aug 12, 2022).

Internet of Things Report. (2022). Available at: https://www.businessinsider.com/internet-of-things-report?IR=T (Accessed Jun 27, 2022).

IoT Security Breaches. (2022). *4 Real-World Examples–Conosco*. Available at: https://www.conosco.com/blog/iot-security-breaches-4-real-world-examples/ (Accessed June 25, 2022).

Jabeen, T., Jabeen, I., Ashraf, H., Jhanjhi, N. Z., Yassine, A., and Hossain, M. S. (2023). An intelligent healthcare system using IoT in wireless sensor network. *Sensors* 23:5055. doi: 10.3390/S23115055

Jabraeil Jamali, M. A., Bahrami, B., Heidari, A., Allahverdizadeh, P., and Norouzi, F. (2020). IoT architecture. *Towards Internet Things*, 9–31. doi: 10.1007/978-3-030-18468-1_2

Javed, S. H., Bin Ahmad, M., Asif, M., Almotiri, S. H., Masood, K., and Al Ghamdi, M. A. (2022). An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). *Electron* 11:742. doi: 10.3390/ELECTRONICS11050742

Jindal, M., Gupta, J., and Bhushan, B. (2019). *Machine learning methods for IoT and their future applications*. In: Proceedings - 2019 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2019, 2019-Janua, pp. 430–434.

Jing, H., and Wang, J. (2022). Detection of DDoS attack within industrial IoT devices based on clustering and graph structure features. *Secur. Commun. Netw.* 2022, 1–9. doi: 10.1155/2022/1401683

Jyotheeswari, P., and Site, N. J. (2020). *Hybrid encryption model for managing the data security in medical internet of things*. Available at: http://acsc.cs.utexas.edu/.

Kamble, A., and Bhutad, S. (2018). *Survey on internet of things (IoT) security issues and solutions*. proceedings of the 2nd International Conference on Inventive Systems and Control ICISC 2018, pp. 307–312.

Kandaswamy, R., and Furlonger, D.. *Blockchain-based transformation: a Gartner trend insight report*. Gartner Research, (2018). Available at: https://www.gartner.com/document/code/352362?ref=grbody&refval=3841665 (Accessed Jun 25, 2022).

Kasim, Ö. (2021). An ensemble classification-based approach to detect attack level of SQL injections. *J. Inf. Secur. Appl.* 59:102852. doi: 10.1016/j.jisa.2021.102852

Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., and Spirito, M. A.. (2013). Demo: an IDS framework for internet of things empowered by 6LoWPAN. In: Proceedings of the ACM Conference on Computer and Communications Security, pp. 1337–1339.

Kesswani, N., and Agarwal, B. (2020). SmartGuard: an IoT-based intrusion detection system for smart homes. *Int. J. Intell. Inf. Database Syst.* 13:61. doi: 10.1504/IJIIDS.2020.10030201

Khanpara, P., Lavingia, K., Trivedi, R., Tanwar, S., Verma, A., and Sharma, R. (2023). A context-aware internet of things-driven security scheme for smart homes. *Secur. Priv.* 6:e269. doi: 10.1002/SPY2.269

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., and Imran, M. (2019). Perception layer security in internet of things. *Futur. Gener. Comput. Syst.* 100, 144–164. doi: 10.1016/j.future.2019.04.038

Khilar, R., Mariyappan, K., Christo, M. S., Amutharaj, J., Anitha, T., and Rajendran, T.., et al.. *Artificial intelligence-based security protocols to resist attacks in internet of things*. (2022).

Kiran, K. V. V., Devisetty, R. N. K., Kalyan, N. P., Mukundini, K., and Karthi, R. (2020). Building a intrusion detection system for IoT environment using machine learning techniques. *Proc. Comput. Sci.* 171, 2372–2379. doi: 10.1016/j.procs.2020.04.257

Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer* 50, 80–84. doi: 10.1109/MC.2017.201

Koohang, A., Sargent, C. S., Nord, J. H., and Paliszkiewicz, J. (2022). Internet of things (IoT): from awareness to continued use. *Int. J. Inf. Manag.* 62:102442. doi: 10.1016/J.IJINFOMGT.2021.102442

Kouicem, D. E., Bouabdallah, A., and Lakhlef, H. (2018). Internet of things security: a top-down survey. *Comput. Netw.* 141, 199–221. doi: 10.1016/J.COMNET.2018.03.012

Kumar Donta, P., Kumar Pareek, P., Kumar Dehury, C., and Anul Haq, M. (2023). DBoTPM: a deep neural network-based botnet prediction model. *Electron* 12:1159. doi: 10.3390/ELECTRONICS12051159

Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X., and Singh, P. (2021). Secure and energy-efficient smart building architecture with emerging technology IoT. *Comput. Commun.* 176, 207–217. doi: 10.1016/J.COMCOM.2021.06.003

Lavanya, M., and Natarajan, V. (2017). Lightweight key agreement protocol for IoT based on IKEv2. *Comput. Electr. Eng.* 64, 580–594. doi: 10.1016/J.COMPELECENG.2017.06.032

Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., and Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. *IEEE Sensors J.* 13, 3685–3692. doi: 10.1109/JSEN.2013.2266399

Lee, R. B., Karig, D. K., Mcgregor, J. P., and Shi, Z.. (2022). *LNCS 2802 - enlisting hardware architecture to thwart malicious code injection*.

Li, L., Hu, X., Chen, K., and He, K. (2011). *The applications of WiFi-based wireless sensor network in internet of things and smart grid*. Proceeding 2011 6th IEEE Conference Ind. Electron. Appl. ICIEA 2011, pp. 789–793.

Liao, C. H., Shuai, H. H., and Wang, L. C. (2018). Eavesdropping prevention for heterogeneous internet of things systems. CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf., 2018-January, pp. 1–2.

Liu, X., and Du, Y. (2023). Towards effective feature selection for IoT botnet attack detection using a genetic algorithm. *Electron* 12:1260. doi: 10.3390/ELECTRONICS12051260

Liu, J., Xiao, Y., and Chen, C. L. P. (2012). *Authentication and access control in the internet of things*. In: Proceedings–32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012, pp. 588–592.

Liu, C., Zhang, Y., Xu, J., Zhao, J., and Xiang, S. (2022). Ensuring the security and performance of IoT communication by improving encryption and decryption with the lightweight cipher uBlock. *IEEE Syst. J.* 16, 5489–5500. doi: 10.1109/JSYST.2022.3140850

Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., and Hayajneh, T. (2018). Security vulnerabilities in bluetooth technology as used in IoT. *J. Sens. Actuator Netw.* 7:19. doi: 10.3390/jsan7030028

Mohanta, B. K., Jena, D., Satapathy, U., and Patnaik, S.. (2020). *Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology, No. 11*. Internet of things (Netherlands). Elsevier B.V., 100227.

Mohanty, J., Mishra, S., Patra, S., Pati, B., and Panigrahi, C. R. (2021). IoT security, challenges, and solutions: a review. *Adv. Intell. Syst. Comput.* 1199, 493–504. doi: 10.1007/978-981-15-6353-9_46

Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., et al. (2020). An efficient lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Futur. Gener. Comput. Syst.* 102, 1027–1037. doi: 10.1016/j.future.2019.09.050

Mosenia, A., and Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* 5, 586–602. doi: 10.1109/TETC.2016.2606384

Naik, N. (2017). *Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP*. 2017 IEEE International Systems Engineering Symposium (ISSE 2017).

Negera, W. G., Schwenker, F., Debelee, T. G., Melaku, H. M., and Feyisa, D. W. (2023). Lightweight model for botnet attack detection in software defined network-orchestrated IoT. *Appl. Sci.* 13:4699. doi: 10.3390/APP13084699

Ni, C., and Li, S. C. (2024). Machine learning enabled industrial IoT security: challenges, trends and solutions. *J. Ind. Inf. Integr.* 38:100549. doi: 10.1016/j.jii.2023.100549

Nirmal, K., Janet, B., and Kumar, R. (2020). Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection. *Peer Peer Netw. Appl.* 14, 2327–2339. doi: 10.1007/s12083-020-00944-z

Noor, M. B. M., and Hassan, W. H. (2019). Current research on internet of things (IoT) security: a survey. *Comput. Netw.* 148, 283–294. doi: 10.1016/j.comnet.2018.11.025

Padhy, S., Alowaidi, M., Dash, S., Alshehri, M., Malla, P. P., Routray, S., et al. (2023). AgriSecure: a fog computing-based security framework for agriculture 4.0 via Blockchain. *Processes (Basel)* 11:757. doi: 10.3390/PR11030757

Vijayakumar, K. P., Pradeep, K., Balasundaram, A., and Prusty, M. R. (2023). Enhanced cyber attack detection process for internet of health things (IoHT) devices using deep neural network. *Processes (Basel)* 11:1072. doi: 10.3390/PR11041072

Raj, A., and Shetty, S. D. (2022). IoT eco-system, layered architectures, security and advancing technologies: a comprehensive survey. *Wirel. Pers. Commun.* 122, 1481–1517. doi: 10.1007/s11277-021-08958-3

Rani, S., Ahmed, S. H., and Rastogi, R. (2020). Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications. *Wirel. Netw.* 26, 2307–2316. doi: 10.1007/s11276-019-02083-7

Rayes, A., and Salam, S. (2022). The things in IoT: sensors and actuators. *Internet Things Hype Real*, 63–82. doi: 10.1007/978-3-030-90158-5_3

Reddy, B. B., Pasha, S. G., Kameswari, M., Chinkera, R., Fatima, S., Bhargava, R., et al. (2024). Classification approach for face spoof detection in artificial neural network based on IoT concepts. *Int. J. Intell. Syst. Appl. Eng.* 12, 79–91.

Reegu, F. A., Ayoub, S., Dar, A. A., Hussain, G., Gulzar, Y., and Fatima, U. (2024). Building trust: IoT security and Blockchain integration. In: 2024 11th international conference on computing for sustainable global development (INDIACom), pp. 1429–1434. IEEE.

Sabahno, M., and Safara, F. (2021). ISHO: improved spotted hyena optimization algorithm for phishing website detection. *Multimed. Tools Appl.* 81, 34677–34696. doi: 10.1007/s11042-021-10678-6

Sadeghi, A.-R., Wachsmann, C., and Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 52nd Annual Design Automation Conference*, pp. 1–6.

Safi, A. (2017). Improving the security of internet of things using encryption algorithms. *Int. J. Comput. Inf. Eng.* 11, 558–561. doi: 10.5281/ZENODO.1130429

Safkhani, M., and Bagheri, N. (2017). Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. *J. Supercomput.* 73, 3579–3585. doi: 10.1007/S11227-017-1959-0

Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., and Boutaba, R. (2022). Man-in-the-middle attack mitigation in internet of medical things. *IEEE Trans. Ind. Inf.* 18, 2053–2062. doi: 10.1109/TII.2021.3089462

Sangaiah, A. K., Javadpour, A., Jafari, F., Pinto, P., Ahmadi, H. R., and Zhang, W. (2022). CL-MLSP: the design of a detection mechanism for sinkhole attacks in smart cities. *Microprocess. Microsyst.* 90:104504. doi: 10.1016/J.MICPRO.2022.104504

Santos, A. L., Cervantes, C. A. V., Nogueira, M., and Kantarci, B. (2019). Clustering and reliability-driven mitigation of routing attacks in massive IoT systems. *J. Internet Serv. Appl.* 10. doi: 10.1186/s13174-019-0117-8

Sarker, I. H., Khan, A. I., Abushark, Y. B., and Alsolami, F. (2023). Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mob. Netw. Appl.* 28, 296–312. doi: 10.1007/s11036-022-01937-3

Savithri, G., Mohanta, B. K., and Kumar Dehury, M. (2022). A brief overview on security challenges and protocols in internet of things application. *IEEE Int. IOT Electron. Mechatronics Conf. IEMTRONICS* 2022:794. doi: 10.1109/IEMTRONICS55184.2022.9795794

Sayakkara, A., Le-Khac, N. A., and Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digit. Investig.* 29, 43–54. doi: 10.1016/j.diin.2019.03.002

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., and Stiller, B. (2022). Landscape of IoT security. *Comput Sci Rev* 44:100467. doi: 10.1016/J.COSREV.2022.100467

Sehrawat, D., and Gill, N. S. (2019). *Smart sensors: analysis of different types of IoT sensors*. Proceeding International Conference Trends Electron Informatics, ICOEI 2019, pp. 523–528.

Selvaraj, S., and Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Appl. Sci.* 2, 1–8. doi: 10.1007/S42452-019-1925-Y/TABLES/1

Sharma, R., Pandey, N., and Khatri, S. K. (2018). *Analysis of IoT security at network layer*. In: 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, 2018-Janua, pp. 585–590.

Sidna, J., Amine, B., Abdallah, N., and El Alami, H. (2020). Analysis and evaluation of communication protocols for iot applications. *ACM Int. Conf. Proc. Ser.* 2020, 257–262.

Singh, N. J., Hoque, N., Singh, K. R., and Bhattacharyya, D. K. (2024). Botnet-based IoT network traffic analysis using deep learning. *Secur. Priv.* 7:e355. doi: 10.1002/spy2.355

Singh, C., and Jain, A. K. (2024). A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network. *E Prime Adv. Electr. Eng. Electron. Energy* 8:100543. doi: 10.1016/j.prime.2024.100543

Sivasankari, N., and Kamalakkannan, S. (2022). Detection and prevention of man-in-the-middle attack in iot network using regression modeling. *Adv. Eng. Softw.* 169:103126. doi: 10.1016/J.ADVENGSOFT.2022.103126

Song, T., Li, R., Mei, B., Yu, J., Xing, X., and Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet Things J.* 4, 1844–1852. doi: 10.1109/JIOT.2017.2707489

Sousa, B., Magaia, N., and Silva, S. (2023). An intelligent intrusion detection system for 5G-enabled internet of vehicles. *Electron.* 12:1757. doi: 10.3390/ELECTRONICS12081757

Sudeendra Kumar, K., Sahoo, S., Mahapatra, A., Swain, A. K., and Mahapatra, K. K. (2018). *Security enhancements to system on chip devices for IoT perception layer*. In: Proceedings - 2017 IEEE International Symposium on Nanoelectronic and Information Systems, iNIS 2017, 2018-February, pp. 151–156.

Telo, J. (2023). Smart City security threats and countermeasures in the context of emerging technologies. *Int. J. Intell. Autom. Comput.* 6, 31–45.

Tewari, A., and Gupta, B. B. (2020). Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Futur. Gener. Comput. Syst.* 108, 909–920. doi: 10.1016/j.future.2018.04.027

Thankappan, M., Rifa-Pous, H., and Garrigues, C. (2024). A signature-based wireless intrusion detection system framework for Multi-Channel man-in-the-middle attacks against protected Wi-fi networks. *IEEE Access* 12, 23096–23121. doi: 10.1109/ACCESS.2024.3362803

Toman, Z. H., Hamel, L., Toman, S. H., Graiet, M., and Valadares, D. C. G. (2024). Formal verification for security and attacks in IoT physical layer. *J. Reliab. Intell. Environ.* 10, 73–91. doi: 10.1007/s40860-023-00202-y

Tufts University and IEEE Circuits and Systems Society (2017). IEEE 60th international Midwest symposium on circuits and systems (MWSCAS): August 6–9, 2017. Boston: MA, USA.

Tukade, T. M., and Banakar, R. M. (2018). Data transfer protocols in IoT-an overview. International Journal of Pure and Applied Mathematics. Available at: https://www.researchgate.net/publication/324152744. (Accessed Jun. 28, 2022).

Ugrenovic, D., and Gardasevic, G. (2016). CoAP protocol for web-based monitoring in IoT healthcare applications. 2015 23rd Telecommun Forum TELFOR 2015, pp. 79–82.

Ullah, I., Noor, A., Nazir, S., Ali, F., Ghadi, Y. Y., and Aslam, N. (2024). Protecting IoT devices from security attacks using effective decision-making strategy of appropriate features. *J. Supercomput.* 80, 5870–5899. doi: 10.1007/s11227-023-05685-3

Vangala, A., Das, A. K., Chamola, V., Korotaev, V., and Rodrigues, J. J. P. (2022). Security in IoT-enabled smart agriculture: architecture, security solutions and challenges. *Clust. Comput. 2022 262* 26, 879–902. doi: 10.1007/S10586-022-03566-7

Velliangiri, S., Amma, N. G. B., and Baik, N. K. (2023). Detection of DoS attacks in Smart City networks with feature distance maps: a statistical approach. *IEEE Internet Things J.* 10, 18853–18860. doi: 10.1109/JIOT.2023.3264670

Wang, Q., Zhu, X., Ni, Y., Gu, L., and Zhu, H. (2020). Blockchain for the IoT and industrial IoT: a review. *Internet Things* 10:100081. doi: 10.1016/J.IOT.2019.100081

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., and Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain–a comprehensive insight. *Symmetry* 13:227. doi: 10.3390/sym13020227

Wei, D., and Qiu, X.. Status-based detection of malicious code in internet of things (IoT) devices. In: 2018 IEEE Conference on Communications and Network Security, CNS 2018 (2018).

Wu, T. Y., Wang, L., Guo, X., Chen, Y. C., and Chu, S. C. (2022). SAKAP: SGX-based authentication key agreement protocol in IoT-enabled cloud computing. *Sustain. For.* 14:11054. doi: 10.3390/SU141711054

Xiao, L., Wan, X., Lu, X., Zhang, Y., and Wu, D. (2018). IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? *IEEE Signal Process. Mag.* 35, 41–49. doi: 10.1109/MSP.2018.2825478

Xu, J., Lin, W., Fan, W., Chen, J., Li, K., Liu, X., et al. (2024). A graph neural network model for live face anti-spoofing detection camera systems. *IEEE Internet Things J.* doi: 10.1109/JIOT.2024.3383673

Xu, Q., Ren, P., Song, H., and Du, Q. (2016). Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* 4, 2840–2853. doi: 10.1109/ACCESS.2016.2575863

Yan, Z., Wang, M., Li, Y., and Vasilakos, A. V. (n.d.). *Cloud-assisted internet of things 28 encrypted data management with Deduplication in cloud computing*. Available at: www.dropbox.com.

Yang, Y. S., Lee, S. H., Wang, J. M., Yang, C. S., Huang, Y. M., and Hou, T. W. (2023). Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token. *Sensors* 23:4970. doi: 10.3390/S23104970

Yassein, M. B., Shatnawi, M. Q., Aljwarneh, S., and Al-Hatmi, R. (2018). *Internet of things: survey and open issues of MQTT protocol*. Proceeding - 2017 International Conference on Engineering MIS, ICEMIS 2017, 2018-January, pp. 1–6.

Yavuz, F. Y., Ünal, D., and Gül, E. (2018). *Deep learning for detection of routing attacks in the internet of things*.

Yugha, R., and Chithra, S. (2020). A survey on technologies and security protocols: reference for future generation IoT. *J. Netw. Comput. Appl.* 169:763. doi: 10.1016/j.jnca.2020.102763

Zargar, S. T., Joshi, J., and Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. *IEEE Commun. Surv. Tutorials* 15, 2046–2069. doi: 10.1109/SURV.2013.031413.00127

Zhang, K. X., Lin, C. J., Chen, S. J., Hwang, Y., Huang, H. L., and Hsu, F. H. (2011). *TransSQL: a translation and validation-based solution for SQL-injection attacks*. In: Proceedings - 1st International Conference on Robot, Vision and Signal Processing, RVSP 2011, pp. 248–251.