Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

A Systematic Review of Security Solutions for IoT Smart Environment with Defense Methods and Mitigation against Various Attacks – Brief Review

Ms.Deepika P.
Research Scholar, SRM Institute of Science and Technology, Chennai.
Dr Agusthiyar R.
Head of Computer Applications (BCA), SRM Institute of Science and Technology, Chennai

Abstract: In the Internet of Things (IoT), heterogeneous actual gadgets and the Web are connected and empower correspondence. Utilizing IoT innovation, an enormous number of gadgets can be interconnected, collecting sensitive information, ranging from industrial controls to medical devices. Increasing dangers in our everyday lives have provoked a worry with security in IoT networks containing an enormous number of items. To guarantee the security of the IoT foundation, proficient, strong cryptographic methods are created and expected to deal with information confirmation, information protection, classification, and respectability. Light-weight operations are being used to reinvent cryptographic solutions. After witnessing the growth of quantum computers, conclude that cryptography based on mathematical problems fails to provide sufficient security. Therefore, solutions for the post-quantum world should be developed that are easy to resist adversarial effects. This paper discusses recent security issues related to IoT addresses a few research questions. There have been several studies recently that propose advanced defense methods for security solutions in IoT environments. Most of examination articles accessible in this field community on the broad field of security solutions in IoT environments. We were able to collect around 80 research articles relevant to security solutions in IoT environments for systematic review in this survey. Our review also covers the open research difficulties and future examination bearings. Furthermore, we talk about the difficulties and headings for creating different protection security arrangements in view of the aftereffects of this review.
Keywords: IoT security, security attacks, intrusion detection system, blockchain, deep learning, machine learning

1. Introduction

The Internet of Things (IoT) is an emerging communication paradigm that connects the physical world with the digital world. I.O.T vision has become a reality thanks to cost reductions in IoT components, improvements in wireless services, improvements in battery life, and improved business models .Furthermore, the implementation of Advances, for example, distributed computing, information examination, Web Convention (IP) based systems administration, nanotechnology, omnipresent registering and other empowering innovations have quickly expanded different IoT applications [2][3]. Accordingly, shrewd urban communities, savvy matrices, brilliant homes, shrewd medical care and more are not future realities. IoT plays an important job in the digitization of society and IoT security issues influence pieces and bytes as well as flesh. Without solid security, assaults and mistakes in IoT-based basic framework will offset any advantages. Then again, protection is likewise vital in IoT. Numerous things that individuals use in their everyday exercises at work and at home are presently associated with the Web. This implies touchy individual information is uncovered on the Web. Tending to protection challenges is similarly as significant as security challenges in IoT. Despite IoT technology benefits for people, society, and industry, its broad reception opens up new security and protection challenges [4]. Getting implanted gadgets and assets is a critical test in the IoT biological system. Moreover, the quick shift from truly secluded frameworks to Web associated, somewhat controlled and observed machines has expanded the assault surface. Also, the asset compelled nature of gadgets in IoT applications makes complex security configuration more testing [5]. A portion of the vital difficulties in building an IoT network are: Overseeing and moving various sorts of data between heterogeneous gadgets is a tremendous test. Such IoT edge gadgets run on various stages and utilize

various conventions to confirm, validate, share information and speak with one another. Overseeing heterogeneous gadgets is testing when the quantity of hubs is enormous [6].

These include network size scaling, information management, device re-location, deployment of new edge devices in older IoT networks, and various keys to authenticate each other while maintaining forward and backward privacy [7][8]. Data sharing includes challenges related to availability, mutual authentication, network traffic congestion, malware attack vulnerabilities, and passive attacks. [9]. Due to hardware heterogeneity, robust IoT algorithms are chosen, a few gadgets perform well, while others perform inadequately because of burden congestion on devices with less computing edge. A lot of energy is squandered in overseeing network blockage and picking the best converter to change over one information configuration to another. Energy-effective meeting key age and delivery mechanisms that perform well with high security under low computational above [10]. The challenge is to reduce the consumption required for communication between different edge devices in an IoT network with the aim of reducing battery power consumption. Network Element Tracking Capability A network element at a sensor node is a collection of physically stolen edge gadgets utilized by aggressors to recover information gathered and put away on the gadget. This frequently occurs in remote sensor organizations, where little or unprotected sensors are utilized. Such gadgets have less equipment security to diminish the organization cost of IoT networks [11]. Edge gadgets should be recognized utilizing the IDs gave during the join stage and the test is to distinguish such edge gadgets while keeping up with the association ordered progression. Assuming the gadget is out of reach, it might should be dismissed for security purposes subsequent to checking impromptu organizations out. Be that as it may, IoT frameworks are helpless against different security goes after like refusal of administration (DoS) assaults and circulated disavowal of administration (DDoS) assaults [12]. Such goes after can make critical harm IoT administrations and savvy climate applications in IoT networks.

An interruption identification framework (IDS) is a security framework that basically works at the organization layer of an IoT framework [13]. A DS carried out for an IoT framework can examine information parcels and create reactions progressively, investigating information bundles with various convention layers at various layers of the IoT organization and IoT climate adjusting to various innovations. IDS is appropriate for IoT-based savvy conditions working under extreme circumstances, for example, low handling limit, quick reaction and high volume of information handling. IoT security is a continuous and basic issue; Thusly, there is a requirement for a refreshed comprehension of the security weaknesses of IoT frameworks and the improvement of moderation techniques.AI procedures are usually utilized in many fields because of their computational power [14]. These strategies basically center around arrangement, grouping and relapse in view of pre-learned highlights in the preparation stage. A peculiarity location model is created to recognize and arrange assaults against digital actual frameworks. Dissimilar to profound learning calculations that robotize the component extraction process, AI calculations give clear guidelines to help independent direction. Profound learning [15] has accomplished great outcomes in different applications including voice acknowledgment, PC vision and normal language handling. The quick advancement of profound learning hypothesis and innovation as of late marks the beginning of the era of artificial intelligence, which opens a new way to create smart IDS.

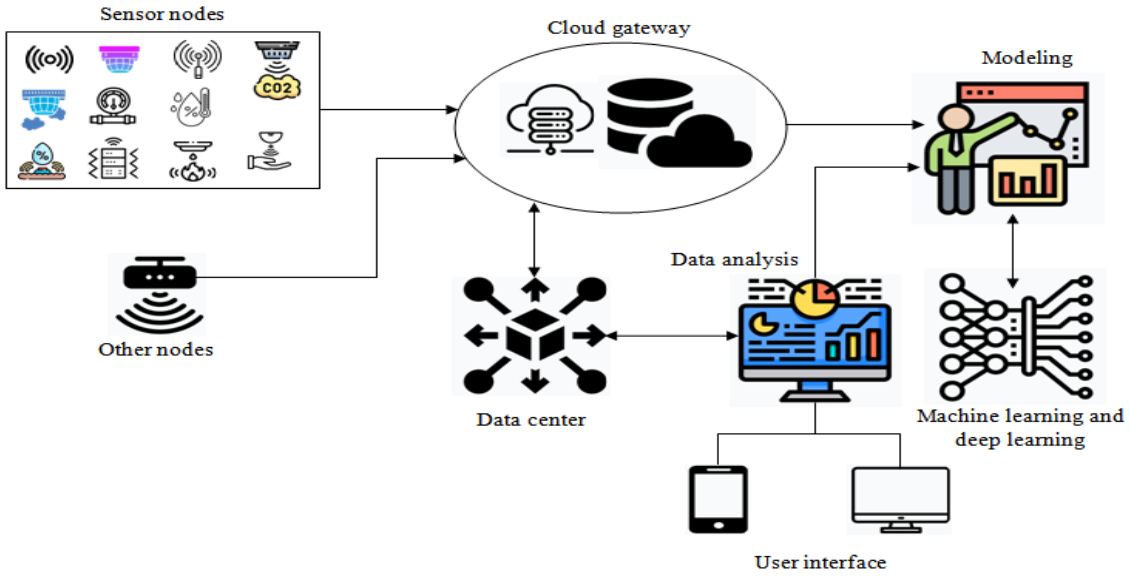

Fig. 1 IoT infrastructure model

2. Background study

The Web of Things (IoT) has extraordinary potential for use in different constant applications. It coordinates sensors, brilliant gadgets, radio recurrence distinguishing proof (RFID) and the Web to frame a canny framework. Goldman Sachs predicts that by 2020, 28 billion shrewd things will be associated with one of a kind organization. The IoT has developed throughout the last 10 years to include everything from sensors to distributed computing delegates to snow/edge processing. Sensors are asset compelled gadgets that are wired or remotely associated with heterogeneous organizations. IoT networks are defenseless against different security, protection and attackers.

2.1 Overview of IoT frameworks

Thanks to the fast improvement of integrated circuit development and far off correspondence advancement, engineers have had the choice to make IoT hubs a lot less expensive and with signal obtaining, information handling and remote correspondence capacities. As displayed in Figure 1, the IoT framework interfaces sensors as well as a few arising innovations. The architecture of IoT is centralized, distributed and decentralized architecture. One of the most difficult issues is IoT application execution and continuous figuring. Distributed computing offers more capacity and ensures information security. In any case, as of late, constant observing IoT applications request handling and figuring at the edge of the organization. Hence immediate measures like monitoring of critical patient health and fire detection can be done. While handling and processing at the edge of the organization utilizing haze gadgets, it is more perilous for assailants on the grounds that their gadgets are lightweight and conventional security doesn't have any significant bearing. While investigating information, procedures, for example, AI have as of late been utilized to make IoT systems more savvy and independent in direction. Different brilliant gadgets are associated with make an application utilizing some standard convention. IoT foundation has security gives that should be addressed to assemble trust among end clients and make the framework sealed. Utilizing the investigation of homegrown and unfamiliar researchers, the IoT framework is by and large separated into three layers: concept, network and application.

- Concept Layer: The focal point of the IoT layer is the different terminal contraptions and correspondence centers. These terminal contraptions can be RFID marks, perusers, cameras and GPS devices. Different sorts of sensors are embedded in the terminal center with the objective that the terminal gadget can detect ecological boundaries. In IoT, the quantity of hubs in the detecting layer is extremely huge and the equipment and programming assets are exceptionally restricted. The detecting layer can gather data from the real world and impart it to

the association layer after easy to-cutting edge change.

- Network Layer: The principal capacity of the association layer is to interface the detecting and application layer. Normal transmission networks incorporate broadcast communications organizations, broadcasting companies, the Web, power transmission organizations, and confidential organizations. Network layer has many access techniques like fiber access, remote access, Ethernet access, satellite access, etc.
- Application Layer: The issues kept an eye on by the application layer are information dealing with and human-PC correspondence. Through the human-PC association point of the application layer, the client can get critical limits from the climate continuously, while simultaneously, a client can give functional directions to the IoT through the application layer to collaborate with the terminal gadget. These platforms work together through middleware technology, virtualization technology, high reliability technology and cloud computing technology to manage, compute, store, analyze and perform mining operations.

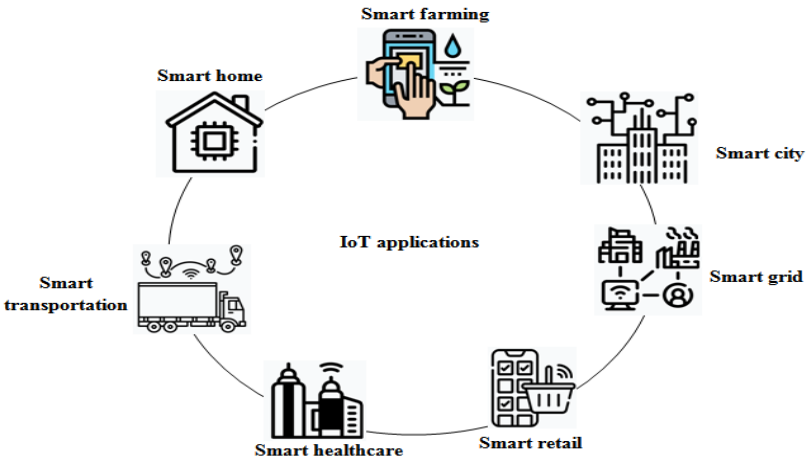

Fig. 2 Applications of IoT

2.2 IoT applications

IoT applications are arising in many fields nowadays. The improvement of a few open source stages, for example, Sky blue IoT Suite, IBM Watson, Amazon Web Administrations (AWS), Prophet IoT, Kaa, Bevy wise IoT stage and cloud-based IoT stage are making versatile IoT applications utilized for modern IoT. Many open source stages are fueled by man-made reasoning (simulated intelligence) and AI (ML) for clever handling and expectation of data. The production of savvy gadgets that can peruse, process and register things makes IoT one of the arising fields. Figure 2 shows the type of application in IoT environment. In these various application areas, IoT has already had an impact on increasing and improving computer performance.

- Savvy home: IoT improves customary home frameworks. Fridge, Brilliant TV, Surveillance Camera, Gas Sensor, Temperature Sensor, Light frameworks can detect and speak with every single indoor climate and interface with the Web through wire or remote.
- Smart Hospital: In a medical care framework, protection is one of the central points of interest, so legitimate security and protection conventions ought to be created to keep the framework secure.
- Smart City: In an ever developing city there are many issues like traffic the executives, squander the board, squander the executives and climate the executives. The city needs answers for screen and control this issue.
- Smart Transport: Transport has become a major issue in the city these days. An intelligent transport system is required. IoT empowers vehicles to gather data from roadside units and obtain travel routes, times and traffic details.
- Savvy Lattice: One of the application areas of IoT is brilliant framework, network framework

computerization should be possible utilizing IoT. Power age and dissemination to shoppers can be checked progressively.

- Smart Retail: The retail industry is also using AI and IoT services to increase productivity, improve store operations and make real-time decisions to manage inventory systems.
- Smart Agriculture: This is a good application area in IoT. In smart farming systems, by implementing sensors to screen soil quality, Water the board, crop development conditions and so on. It works on rural effectiveness by decreasing time and cost.

2.3 Security attacks in IoT

A cyber-attack is a breach of a computer with malicious intent. Examples include disavowal of administration and data fraud. IoT gadgets are "brilliant" actual articles with programming and equipment that associate with different gadgets or organizations and play out specific registering capabilities. Notwithstanding, two normal classes of IoT security assaults are caricaturing assaults and forswearing of-administration (DoS) assaults. Ridiculing assaults are aimed at different pieces of the organization, from moderate doors to end gadgets. With regards to IoT, such middle people are much of the time brilliant center points that associate far off gadgets to neighborhood organizations. Much of the time, these entryways don't perform confirmation prior to laying out contact with end gadgets. Therefore, an aggressor can parody at least one believed gadgets and get close enough to other IoT endpoints associated with that middle gadget.

Denial of service (DoS) attack: It is for the most part connected with vindictive goal. These sorts of assaults render networks unusable for clients by making a surge of parcels to close down significant assets like DNS servers or HTTP web servers.

- Convention assault: It is one of numerous ways that programmers can endeavor to take information from your organization or framework. They include a programmer interfacing with organization or gadget utilizing convention orders. One of our greatest worries while discussing convention assaults is something many refer to as man-in-the-center assaults.
- Pantomime assault: It is a sort of digital assault wherein a noxious entertainer embraces or mirrors one more client's personality to acquire unapproved admittance to safeguarded network assets. Frequently, assailants attempt to mimic a significant level leader to sidestep security controls or compromise organization information.
- Derivation assault: It focuses on a confidential key. The aggressor looks for values in memory that compare to unused pieces of information put away on blockchain and afterward attempts to figure out that information. In the event that fruitful, an aggressor would figure out how a client made their confidential key and might actually utilize it to take assets from different clients. It is essential to take note of that most refined malware can finish beast force assaults without help from anyone else.
- Accessibility assault: Acquiring unapproved admittance to a PC or network is utilized. The assailant enters utilizing a secondary passage, which should be possible through telnet, ssh, FTP administration, unreliable remote associations, or by speculating passwords.

3. Research methodology

Research methodology is the process of systematically conducting research. It involves a theoretical analysis of all theories related to a particular field. It generally includes the concepts of phase, sampling, and qualitative and quantitative methods. Key Data Collection Features of this study: Key data collection procedures and research methods for data collection. The following section provides an efficient survey of safety efforts in the IoT literature. To do this, we first develop a search prism framework that highlights keyword selection, search strategies, search sources, and filtering. A systematic review is needed to identify, categorize and compare existing research on sign language recognition. In the last decade, there have been many studies on security in IoT, attacks in IoT, IDS schemes for IoT, crypto techniques for IoT, blockchain for IoT, machine learning techniques for IoT, and deep learning techniques for IoT. But none of these lead to a formal literature review process. This paper provides a comprehensive review to systematically classify and compare all available methods and techniques related to security development in IoT. The

following research questions were formulated to conduct a systematic review of the literature.

RQ1: What are the attacks mostly present in the IoT environment and how IDS resist it.

RQ2: What are the most commonly used feature extraction in the process of IDS.

RQ3: What is the importance of lightweight cryptography in IoT environment and how it improves system performance?

RQ4: What is the role of ML and DL in intrusion detection system in IoT environment and how to improve detection rate?

RQ5: What is the most commonly used metric for standardization and which IDS scheme are mostly suitable for future study.

3.1 Keywords selection

The first step in this systematic literature review is the selection of keywords. Here we divide our research criteria into six categories: IoT, Attacks on IoT, IDS for IoT, Crypto Techniques for IoT, Blockchain for IoT, Machine Learning for IoT, and Deep Learning for IoT. This increases the chances of finding a significant number of relevant keywords. We want to focus on AI and profound learning methods and analyze several related acronyms and keywords to include in key searches.

3.2 Search strategy

The following terms are used to generate search terms:

- Identify keywords that match the requirements written in the title
- Find all alternatives of language and meaning.
- Boolean operator should be used to get terms (or all) entries or to join similar terms.
- The logical operator, which is best, should be used to register all terms and join the main terms.

Database searches look for keywords from specific categories (such as machine learning for IoT and/or deep learning for IoT) to generate a comprehensive list of these keywords. Also, we use the AND function to extract some documents from the database records. After choosing a strategy, we need to capture a user timeline of article selection and several outcome measures, including article titles, publication years, abstracts, author names, publisher information, references, and links to full articles.

3.3 Search sources

There are nine electronic databases for basic research (SpringerLink, IEEE Explorer, ACM Digital Library, Science Direct, Wiley, InderScience, TandF, Hindwi and Google Scholar). Other important sources such as nature, entomology and computational biology were not considered as they were fully covered by the selected data sources. Search for terms in nine databases before searching journals and conference articles. Different database search engines use different search strings to rank different records. Search is limited to 1998 to 2021. Search the top five databases for topics and keywords recommended by Google Scholar. Search full-text titles and millions of unrelated entries.

3.4 Filtering documents

Fig. 3 shows the PRISM flow of the relevant literature review on security in IoT, attacks in IoT, IDS schemes for IoT, crypto methods for IoT, blockchain for IoT, machine learning techniques for IoT and deep learning techniques for IoT. Between 2010 and 2022, an initial 4,123 records were collected. Because we collected data from two different databases, duplicate articles were automatically removed from the system, leaving 840 entries for further analysis of titles and abstracts. The several papers and abstracts related to sign language recognition, sign language classification, and different types of sign languages were excluded after screening. The remaining 574 articles were assessed for full-text review. This guide has been carefully reviewed by two independent reviewers with expertise in the field. Articles related to sign language recognition and sign language classification were rejected. If consensus could not be reached, the comments of a third reviewer were taken into account. Finally, 241 articles were evaluated for the final systematic review and analysis. Out of these 241 articles, 80 articles are about our contribution.

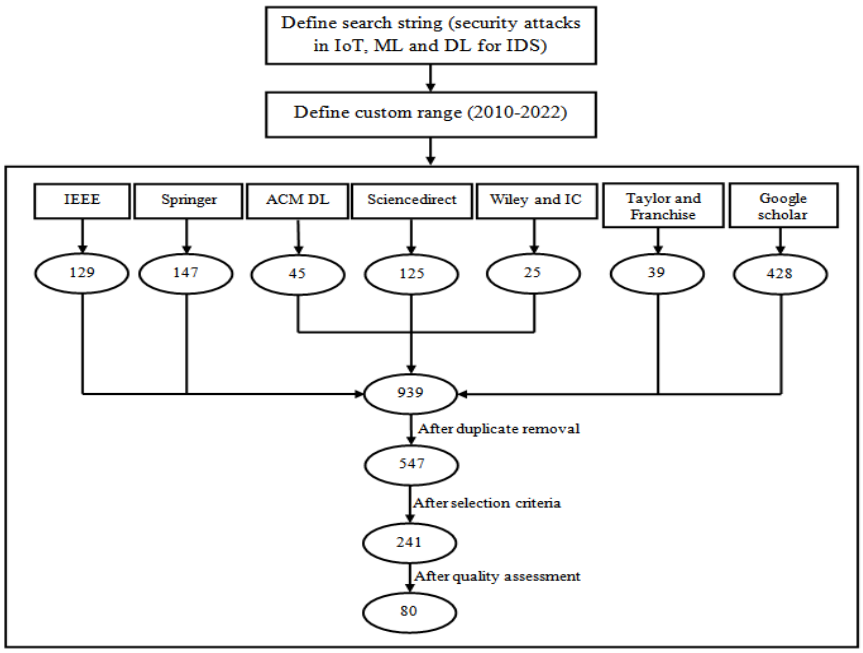

Fig. 3 PRISMA flowchart for our systematic literature review

4. State of art techniques

The quickly developing web associated gadgets, going from little sensors to cloud servers bring the idea of the IoT where things allude to little articles like candy machines, electronic apparatuses, cameras, savvy bulbs, brilliant locks, indoor regulators, and some more. IoT changes these articles from customary to savvy utilizing the fundamental rule of omnipresent figuring, correspondence conventions and applications. According to a systematic review, recent technologies have significantly impacted security measures for IoT environments. Current work mainly focuses on blockchain-based IDS schemes to improve security in IoT environments. As a result, our systematic review provides the best solution for choosing the appropriate IDS scheme for the respective attacks. Figure 4 describes our systematic literature review based on various subcategories of IoT attack types and traditional IDS schemes. Lightweight crypto based IDS projects, blockchain based IDS projects, machine learning based IDS projects and deep learning based IDS projects.

4.1 Review on security attacks in IoT [16]-[30]

Yu et al. [16] have proposed the mix of organization inactivity and leak-based connectivity exposes the vulnerability of IoT infrastructure to deliberate attacks. Deliberate attacks pose a serious threat to network operations as they disrupt the network by crippling few hubs, subsequently upsetting IoT activities. A combination based security framework is utilized to relieve the harm brought about by such assaults, where every hub gives the base neighborhood consequence of the assault forecast to the combination community. Web based and Digital Actual Framework (CPS)- based network resilience are analyzed separately to represent the future IoT infrastructure. Zhang et al. [17] have proposed Cyber Attacks and Security Schemes in IoT. Define Sybil attacks: SA-1, SA-2, SA-3, depending on the capabilities of Sybil attackers. Duy et al. [18] have proposed The issue of shielding against assaults on honeypot-empowered networks is tended to by a game-hypothetical model of aggressor and safeguard trickiness. An assailant attempts to trick the protector utilizing different assaults going from dubious appearances to basic activities, while the safeguard can involve honey pots as an instrument to trick the aggressor. The issue is planned as a Bayesian round of fragmented data, distinguishing equilibrium for a single shot game and rehashed game renditions

Xu et al. [19] have proposed a Smart Security Mechanism (SSM) is proposed to protect against new flow attacks. SSM uses SDN's south and north interfaces and provides an inexpensive way to monitor new-flow attacks through asynchronous

message reuse on the control link. The monitor mechanism distinguishes new flow attacks from normal flow bursts by observing the flow entry success rate. Based on monitoring results, SSM uses dynamic access control mechanisms to mitigate new flow attacks by understanding the behavior of security middleware in IoT. A dynamic access control mechanism can prevent the flow of attacks on their access switches. Extensive simulation and test bed-based experiments have been conducted, and the corresponding results confirm the feasibility of our claims. Li et al. [20] have proposed Potential threats of man-in-the-middle attacks on open flow control channels are explored. Attack models in the IoT-Fog framework and use attack demonstrations to show the extreme effects of such attacks. Also, we recommend a light resistor with a bloom filter. We implement a prototype of this method to investigate hidden packet changes. Yu et al. [21] have proposed A key-based Advanced Encryption Standard (AES) technique is proposed to prevent leakage of secret keys stored in switch boxes under Communication Power Analysis (CPA) attacks. XOR gates based on wavelet dynamic difference logic (WDDL) are used to hide intermediate data with high correlation with erroneous keys in the reconstruction stage. After executing the invalid key and generating the reconstruction step using WDDL, the minimum metric-exposure value to enable the proposed light mask AES engine against CPA attacks is greater than 150 million. Qiu et al. [22] have proposed a Secure Time Synchronization Model for Colossal Extension IoT. A center point uses its father center and granddad hub to distinguish malignant hubs. Utilizing the model, we can make a Bounce with a synchronized Jump spreading over tree geography utilizing reference hubs. The Protected Time Synchronization Convention (STSP) was then evolved to battle copy timestamps following the safe model. Zhang et al. [23] have conducted a new algorithm for retagging in IoT is robust against malicious attacks. TW-TOA localization algorithm suffers performance degradation due to such attacks. The scriptures demonstrate the use of hearsay information. To calculate the maximum likelihood estimate (MLE) for the location of the tag. Lin et al. [24] proposed a this is avoidable protocol spectrum management, a common type of security risk despite local implementation limitations.

Table 1 Summary of research gaps with respect to security attacks in IoT

Ref.	Methodology	Attacks	Techniques used	IoT application
[16]	Defend intentional attack in IoT	Sybil, DoS, DDoS	Zero-sum game	Cloud
[17]	Sybil attacks defenses in IoT	Sybil	Social graph network	Smart home
[18]	Deceptive attack defense in IoT	DoS and DDoS	Bayesian game	Smart city
[19]	New-flow attack defense in IoT	DoS and DDoS	SSM	Cloud
[20]	Man in center assault guard in IoT	Man in center	SDN	Smart home
[21]	CPA attack defense in IoT	CPA attack	WDDL XOR-AES	Smart city
[22]	Time synchronization protocol against fake timestamps	DoS and DDoS	Secure time synchronization protocol (STSP)	Smart city
[23]	Mitigating localization spoofing attacks for IoT	Spoofing	M-SLOT, D-SLOT	Smart home
[24]	Authentication protocol for IoT	PUEA	T2DAP	Cognitive radio sensor networks
[25]	Low-cost security of IoT	Known-Plaintext	Rakeness compressed sensing	Smart home
[26]	Jamming mitigation of IoT	Jamming	Game equilibrium	Smart city
[27]	DDoS attack mitigation of IoT	DDoS	Optimal CNN	Smart home

[28]	Buffer overflow attacks in IoT	Buffer overflow	CDNN	Cloud
[29]	Routing attack mitigation in IoT	Routing attack	RDNN	Smart city
[30]	Sparse estimation attack in IoT	Spoofing	Privacy-aware controllable compressed data	Cloud

Principal user emulation attack (PUEA) is one of the most destructive attacks in cognitive radio sensor networks. Mangia et al. [25] Only compression sensitive level technology is optimized for known plaintext attacks to maximize compression performance using a hackiness-based design. Despite such trade-offs, detection-based compressed sensing exhibits significant robustness to scientific attacks. This is fully justified by some theoretical considerations and compromises security to some extent as an attacker has access to information. Through the numerical evidence presented, it can be shown that the loss of security does not prevent this method from performing a remarkably robust scientific attack.

Tang et al. [26] have proposed an Anti-Reactive-Jamming Transmission Strategy for IoT Exploitation of Jammers' Inherent Vulnerabilities. In particular, since reactive congestion is based on detecting systematic exchanges, System users can trade off transmission power between received signal-to-interference-plus-noise ratio (SINR) and detection probability. Meanwhile, the jammer intelligently determines the jamming power based on monitoring frame exchanges. Yin et al. [27] have proposed a common architecture for software-defined IoT based on the SDx paradigm. The architecture includes SD-IoT controllers, SD-IoT switches and IoT gateways, and a controller pool of IoT devices. In an algorithm to detect and mitigate DDoS attacks using the SD-IoT architecture, the cosine similarity of the packet-in message rate vectors at border SD-IoT switch ports is used to determine whether it exists. Xu et al. [28] have proposed an architecturally optimized security equipment configuration is proposed to recognize cradle flood assaults. A piece of the plan is checking and testing the components used to screen the exhibition of the program. One more protected tag is approval, which is utilized to confirm the characteristics of every memory fragment. Programmed extraction apparatuses separate the checking model and security labels for every memory fragment at gather time. At runtime, the planned equipment takes a gander at its dynamic execution follow and checks whether the follow matches the permitted conduct. Raoof et al. [29] have directed a RPL portrays its known assaults and proposes relief strategies to battle these assaults. Wang et al. [30] have proposed a Privacy protection of unpublished data when data is published in IoT. CS technology is in place to ensure that data privacy requirements are not compromised in a privacy-aware controlled compressed data release program. The reconstruction error of CS inherently increases the privacy protection ability against rare prediction attack by unknown individuals. Table 1 describes the summary of research gaps which gathered from the state-of-arts works related to security attacks in IoT.

4.2 Review on IDS scheme in IoT [31]-[40]

Al et al. [31] have proposed a methodology for capturing and analyzing the exchange of assault and safeguard methodologies for interruption recognition in computerized circulated IoT Frameworks. To form every hub should partake in light interruption location of adjoining objective hubs. Subsequently, every great hub plays a bunch of guarded procedures to dependably safeguard the framework, while every terrible hub plays a bunch of hostile methodologies to accomplish its objectives. Alhakami et al. [32] have proposed a peculiarity based IDS issue, completely Bayesian-based approach for a summed up Gaussian blend model with limitless limitations. A significant component of the created model is that it incorporates an element choice technique to keep superfluous highlights from compromising the demonstrating system. The decision of the Bayesian induction strategy is propelled by the way that it permits us to abstain from under fitting and overfitting, formalize our earlier information, and express our vulnerability through a likelihood dispersion. Chau et al. [33] have conducted a IDS is an attack-defense game for autonomous IoT devices work together to solve problems. An analytical model is used to identify situations

where malicious nodes have no incentive to attack in the attack-defense game of intrusion detection. Petri net model is used to define system failure scenarios as input and analyze the effect of attack-defense behavior on system reliability. Abdollahi et al. [34] have proposed aping of death as a digital protection assault intended for IoT Organizations Aggressors purposefully increment the length of communicate bundles which exhausts network resources. IDS are designed to reduce the ping of lethal attacks, detect attacks, and are embedded in network gateways to filter out packets of excessive length. IDS relies on integer optimization problem to minimize the probability of false alarms and keep the missed detection probability below a desired level. Problem solved using search method. Nimbalkar et al. [35] have proposed highlight determination for IDS use data gain (IG) and gain proportion (GR) with highlights positioned in the top half to distinguish DoS and DDoS assaults. The predetermined framework include subsets are gotten utilizing addition and association procedure on the subsets got by the top half IG and GR highlights. The proposed strategy was assessed and approved by JRip classifier on IoT-BoT and KDD Cup 1999 datasets, independently. It beats the first list of capabilities and conventional IDS with 16 and 19 highlights on the IoT-BoT and KDD Cup 1999 datasets, separately. LIU et al. [36] have proposed molecule swarm enhancement based angle plunge for interruption discovery (PSO-LightGBM). PSO-LightGBM is utilized to remove elements of the information, recognize and distinguish vindictive information, and feed them into a one-class SVM (OCSVM). UNSW-NB15 dataset is utilized to approve the interruption identification model. Kalnoor et al. [37] have proposed a crypto based solution for IoT network and improvement remains a major challenge for research, which is viewed as a restricted asset for the security of IoT gadgets. The performance metrics of the proposed model are tabulated with a FAR of 19%, the FAR for other algorithms is higher, which reduces the intrusion detection accuracy. The precision of the got proposed model is 100 percent contrasted with different calculations with less exactness. Hu et al. [38] have handles an attribution problems do not appear in sample data to detect intrusions.

DS framework is for 5G and IoT networks in light of blemished piece with multi-part K-implies. Exploratory outcomes show that IDS technique accomplish high-precision bunching when test information is deficient. All things considered, it has a few hindrances regarding execution and processing large amounts of data. Basati et al. [39] have proposed a lightweight framework based on asymmetric parallel auto-encoder (APAE) which uses extended and simplified transform channels to separate neighborhood and long-range data around individual qualities in an element vector. There is likewise a stage auto-concentration and channel auto-center module to separately work on nearby and long-range highlights. The APAE approach has a lightweight and reasonable system for continuous assault recognition and gives superb speculation execution. Jabbar et al. [40] have proposed an auto encoder for IDS plot. Computationally costly auto encoders make it trying to use for interruption identification in cloud or organizations of gadgets with less assets than information. Table 2 describes the summary of research gaps which gathered from the state-of-arts works related to IDS scheme in IoT

Table 2 Summary of research gaps with respect to IDS schemes in IoT

Ref	Methodology	IDS scheme	Feature extraction	Attacks	IoT application
[31]	Defense strategies for IoT	Stochastic Petri Net (SPN)	Iterative computational	Probe, sybil	Smart retail
[32]	Anomaly based intrusion detection	Nonparametric Bayesian	Markov chain Monte Carlo	DoS, DDoS	Smart home
[33]	Attack defense for IoT	Stochastic Petri Net (SPN)	WSO	Byzantine	Cloud
[34]	Defense strategies for	IDS-CNN	PSO	Ping of death	Smart home

	ping of death attacks in IoT				
[35]	IDS for IoT	SVM	IG-TFP-FS, GR-TFP-FS	DoS, DDoS	Cloud
[36]	Defense strategies for IoT	One-class SVM	PSO-LightGBM	DoS, whomhole	Smart city
[37]	IDS for IoT	SVM	Markov model	Man in middle	Smart city
[38]	IDS multiple-kernel clustering	Multiple-kernel K-means clustering (MKKM)	PSO	DoS, DDoS	Cloud
[39]	IDS for IoT	Asymmetric parallel auto-encoder (APAE)	CNN	DoS, DDoS	Smart environment
[40]	IDS for IoT	Adaptive ensembles of auto encoders	Kitsune 23 features	Man in the middle, DoS	Smart city

4.3 Review on security attacks addressing using lightweight crypto techniques [41]-[50]

Tedeschi et al.[41] have proposed a lightweight additive-free certificate-less key contract protocol suitable for integration with stack and managed IoT devices. Key contract protocol features certified include: temporary cryptographic content; support for intermediate connection with TTP; light reeking operations; Robustness against impersonation attacks even if information stored in TTP is leaked. Wazid et al.[42] have proposed a growing area of research on cloud-based IoT environments. A lightweight confirmation framework for getting a cloud-based IoT climate (LAM-CIoT) addresses the security issues it requires. Thorough security investigation of LAM-C IoT utilizing formal security utilizing ROR model, formal security testing utilizing AVISPA device and casual security additionally show that LAM-CIoT is helpless against a few known assaults. Can handle what is needed. LAMC IoT supports adding new IoT sensors to the network after the initial deployment, password facility furthermore, biometric update stage. LAM-CIoT jam obscurity and non-detectability highlights. LAM-C IoT is contrasted and firmly related plans used in IoT environments, and the analysis shows that LAM-CIoT outperforms existing schemes. Sadhukhan et al.[43] have proposed The ECC-based three-factor far off client confirmation plot deals with brilliant gadgets and protects the communicating user's privacy and data confidentiality. Several cryptographic attacks were analyzed and the proposed scheme was made resistant to those attacks. Biswas et al.[44] have a lightweight encryption strategy called LRPC is proposed in this work for asset compelled IoT gadgets, which can give information security at a delicate level. LRBC joins the primary benefits of the Replacement Change Organization (SPN) and the Feistel system to accomplish better security. This algorithm consumes a minimum power of 11.40µW and covers an area equal to 258.9 gates. Also, in-depth security investigation shows that the proposed conspire serious areas of strength for ensures protection from different assaults. Likewise, the typical torrential slide impact of LRBC was viewed as 58% and 55.75% for plain text and key individually. Rashidi et al. [45] have proposed an Inverse- based S-box with preferred equipment execution over AES S-box with comparative cryptographic properties. The S-box computation essentially comprises of two stages, field reversal and relative change. The inborn S-box uses compelling relative change with low district resources and low essential way delay (CPD). The sub-blocks of the S-confine are completed light of the field pivot compelling circuit in the F24. Multiple gates are implemented in the architecture with 2-input NAND and 2-input NOR doors to lessen inactivity and area. NING et al. [46 have proposed The framework specifies performance, physical and safety requirements through widely accepted standards such as NIST and ISO/IEC 29192 International Standards Organization standard for evaluation criteria. Two decision-making methods, CRITIC and TOPSIS, are used to evaluate alternatives (codes) against

defined evaluation criteria. Hammi et al.[47] have proposed a new approach to generating OTPs based on ECC and isogeny. We expanded the idea of OTP and utilized it to produce another key utilized for each trade between an IoT gadget and a server. Moreover, our methodology enjoys the benefit of not depending on timestamps, for example, counters or connections OTP-type component. This new plan doesn't need challenge/reaction taking care of, for example, non-concurrent OTP-type instruments. Choudhury et al. [48] have proposed an elective lightweight plan is proposed for character protection of IoT gadgets in 5G versatile organizations. Another venture called 'HashXor' requires just two hash activities and three XoR tasks for an IoT gadget to accomplish its objective. The task is completely safe through security investigation and precise examination. Through execution time examination on ATmega328P central processor, this plan is viewed as computationally effective contrasted with ECIES and a few late recommendations. the field. Hence, in this paper Weaver proposes a plan called 'HashXer' which utilizes just lightweight 'Hash' and 'Xer' capabilities to safeguard character protection of IoT gadgets. Yaser et al.[49] have proposed another lightweight confirmation and approval conspire for ongoing information access in IoT cloud-based conditions called LMAAS-IoT. The endeavor is expressly intended for conveyed and high-volume frameworks, making a protected and proficient arrangement that meets current prerequisites. LMAAS-IoT is light as far as calculation and correspondence costs, utilizing just XOR tasks and cryptographic hash operations. Kumar et al.[50] havepresenteda lightweight cipher based on military operations, the Feistel system is a combination of the Splendid and Simon structures, thus the name Briti. A code encodes a 32-bit plaintext with a 64-cycle key. The arrangement was reenacted using Xilinx Vivado and in view of Nexys-4 DDR Artix-7 and Basys-3 Artix-7 FPGA family to assess power and timing and exhibit the security of the proposed calculation. All criteria are met Table 3 illustrates a summary of research gaps collected from state-of-the-art works related to lightweight crypto techniques for IoT.

Table 3 Summary of research gaps with respect to lightweight crypto techniques for IoT

Ref	Methodology	Lightweight crypto	Attacks	Database	IoT application
[41]	IDS for IoT	LiKe	Sybil, DoS, DDoS	NSL-KDD	Healthcare
[42]	IDS for LAM-CIoT	LAM-CIoT	DoS, DDOS	KDDCup99	Cloud
[43]	IDS for ECDH	Lightweight ECC	Man in middle	NSL-KDD	Agriculture
[44]	IDS for LRBC	LRBC	DoS, DDOS	CICDDoS2019	Smart city
[45]	IDS for CLEFIA	S-box	Sybil, DoS, DDoS	CIDDS-001	Smart Education
[46]	IDS for CRITIC	MCDM	Routing	KDD1999	Smart Agriculture
[47]	IDS for IoT	Lightweight ECC	Wormhole, DDoS	Darpa98, KDD99	Transportation
[48]	IDS for IoT	HashXor	Internal, wormhole	NSL-KDD	Smart city
[49]	IDS for LMAAS	LMAAS-IoT	Man in middle	CIDDS-001	Transportation
[50]	IDS for BRISIL	BRISI	Spoofing, Sybil	KDDCup99	Jamming

4.4 Review on security attacks addressing using blockchain [51]-[60]

Rahman et al.[51] have proposed a blockchain-based framework to help security and protection based spatiotemporal brilliant agreement administrations for a practical IoT-empowered shared economy in uber shrewd urban communities. Simulated intelligence creates significant advanced examination to process and catch basic occasion data, and stores results in blockchain and decentralized cloud archives to empower sharing of monetary administrations. The structure gives a reasonable impetus framework that can really uphold secure savvy city administrations like sharing economy, brilliant agreements, blockchain and digital actual connections with IoT. Yohan et al.[52] have proposed a secure and genuine blockchain-based

firmware update structure for IoT conditions. It gives a protected shared confirmation process with each new firmware rendition delivered by the particular gadget maker and gives ideal refreshed firmware to IoT gadgets. There are four cycles in this firmware update engineering: firmware update contract creation, pariah firmware update contract creation, push update strategy, and pull update technique. Six related conventions are intended to help the four cycles. The presentation and security strength of the proposed firmware update design are assessed. Ren et al.[53] have proposed a Blockchain innovation to propose a trust association framework reasonable for conveyed IOMT. A safer and versatile trust system is laid out without expecting the presence of outsiders or these CAs being trusted. Shi et al.[54] have conducted a blockchain-based admittance control plot for safeguarding security in disseminated IoT, formalizes the circulated design and conventional brought together access control model in IoT. Utilization of lightweight encryption calculation guarantees security. In BacS, all entry control trades are encoded and re-designed by the space the board server. Khalid et al.[55] have proposed a decentralized confirmation and access control approach for lightweight IoT gadgets is proposed and applied to huge scope situations. The framework depends on haze figuring innovation and public blockchain idea. The outcomes acquired from the examinations show the better exhibition of the framework contrasted with the cutting edge blockchain-based confirmation strategies. An assault model is characterized to assess our methodology and confirm its capacity to meet these necessities. Future work will focus on developing lightweight consensus protocols that recommend miners based on their trust value to avoid the enormous energy costs required for PoW to verify each block.

Sahay et al.[56] have presented a layered model of IoT guiding security to separate the shortcomings related with each step of the directing framework. We explore how the in born elements of blockchain-upgraded steering security can be utilized in IoT-LLNs. Thusly, we propose a blockchain-based system with brilliant agreements to produce constant cautions to really recognize sensor hubs associated with corrupting LNL configuration information. Hameed et al.[57] have proposed an effective decentralized blockchain-based confirmation plot pointed toward accomplishing secure validation for IoT gadgets utilizing a symbolic instrument. Displaying, examination, and approval of this task using huge level Petri nets (HLPNs) and the Z3 SMT arrangement are introduced to confirm model cases perpetually. Shao et al.[58] have conducted IBE-BCIOT, a new cross-chain communication method for blockchain communication problem in IoT environment. Among them, IBE-BCIOT adopts a cross-chain notary system to securely communicate between numerous IoT blockchains or IoT blockchains and non-IoT blockchains. The IBE-BCIOT technique chooses intermediary hubs of each blockchain among various blockchains. Likewise, it gathers the intermediary hub's ID as a public key and sends it to the cross-chain legitimate authority. A cross-chain legitimate authority public cycles the relating private key through the IBE procedure and securely returns it to the intermediary hub, empowering secure and efficient communication between blockchains. Ammi et al.[59] have proposed a Blockchain-based answer for secure savvy home frameworks utilizing incorporated Hyper ledger Texture and Hyper ledger Writer. This arrangement is intended to defeat security limits detailed in regularly utilized blockchain methods. This mapping provides a customized, purpose-built solution that meets the security needs of IoT-based brilliant homes. Hossein et al.[60] have proposed the blockchain-based approach allows users to control access to their data and share their health data with medical personnel. To build versatility and execution, we gathered BC network hubs into different bunches and relegated every client to a particular group for information capacity and access strategies. BCHealth permits information proprietors to characterize the entrance approaches they need on their protection delicate wellbeing information. BCHealth has two separate organizations for putting away access arrangements and information exchanges.

Table 4 Summary of research gaps with respect to blockchain techniques for IoT

Ref	Methodology	Blockchain	Attacks	IoT application
[51]	IoT-based cognitive edge	DNN, CNN Blockchain	DoS, DDoS	Smart city
[52]	Secure blockchain for IoT	Optimal blockchain	Impersonation, man-in-the-middle, replay	Smart city
[53]	Blockchain-based trust establishment mechanism	CA of multiple-PKI trust	Anti-replay attack	Smart home
[54]	Blockchain-based access control scheme	SEA-Blockchain	Destruction, administrator	Smart city
[55]	Decentralized lightweight blockchain IoT	Decentralized authentication Blockchain	Wormhole	Smart communities
[56]	Blockchain for IoT-LLNs	Attack graph Blockchain	Routing	Smart Contract
[57]	Blockchain based decentralized authentication scheme	High level Petri nets	Jamming	Smart transport
[58]	Cross-chain correspondence system of blockchain in IoT	IBE-BCIOT	Routing	Smart health
[59]	Blockchain-based architecture for IoT	Blockchain with mapping	DoS, DDoS	Smart home
[60]	Blockchain-based privacy-preserving for IoT	K-means cluster blockchain	DoS, DDoS	Smart healthcare

4.5 Review on security attacks addressing using machine learning [61]-[70]

Liu et al.[61] have proposed the quantity of tests and the pursuit time are a few significant elements that influence the presentation of the calculation. The principal factors influencing this calculation are: Investigation is finished through reproduction. Trial results show that the productivity and exactness of the interruption recognition calculation step by step decline as how much information increments. Contrasted with Bayesian calculation and brain network calculation, it actually has better hunt execution. With the consistent improvement of applicable exploration, the new interruption recognition models of IOT will build to an ever increasing extent, and the assessment file will keep on developing. In additional exploration, different markers and new highlights of IOT can be added to work on the interruption detection model. Verma et al.[62] have presented a Potential application of machine learning arrangement calculations to safeguard IoT against DoS assaults. Oddity based IDS will be widely contemplated to foster classifiers. Friedman and Nemenyi tests were utilized to investigate genuinely massive contrasts between orders. Raspberry Pi is utilized to assess the reaction season of the classifier on IoT explicit equipment. Rahman et al.[63] have proposed a cutoff unified IDS for asset compelled gadgets by proposing two techniques, semi-endlessly disseminated, that consolidate elite execution include extraction and determination with plausible mist edge cognizance examination. Collaborative models perform feature selection and multi-layer perceptron classification separately, after which the output coordinates are combined with edge or fog to produce the final result. Jyoti et al.[64] have presented a model in the context of these issues and to propose a better communication model, specifically the Energy Aware Smart Home (EASH) framework. Types of communication failures and network attacks are analyzed in EASH. Rahman et al.[65] have proposed to apply successful element choice strategies to further develop interruption

discovery utilizing AI procedures. Unified IDS utilizes profound element extraction, highlight choice and order to prepare models to identify pernicious and surprising action in rush hour gridlock. Profound element extraction involves profound learning methods of fake brain networks as solo auto-encoders to create extra highlights for the traffic.

Table 5 Summary of research gaps with respect to machine learning based IDS scheme for IoT

Ref	Methodology	Feature extraction	DL technique	Attacks	Database	IoT application
[61]	IDS for IoT	SFC	WSN	DDOS	NSL-KDD	Agriculture
[62]	IDS for IDSs	PCO	FCM	DoS	CIDDS-001	Healthcare
[63]	IDS for IoT	PCA	MLP	FGSM	CIDDS	Smart city
[64]	IDS for EASH	DDQN	MLP	DDOS	KDD CUP 99	Smart Education
[65]	IDS for IoT	SVM	ANN	Jamming	AWID	Cyber attacks
[66]	IDS for MADP-IIME	PCA	HCAPN	DOS	Benchmark	Agriculture
[67]	IDS for IoT	CNN	LSTM	Routing attack	ICS,NSL-KDD	Cyber attacks
[68]	IDS for IoT Networks	MKC	K-NN	Implementation	KDD1999	Smart city
69]	IDS for GWO–PSO–RF	PSO	IDC	Buffer overflow	CICIDS-2017,KDDCup99	Healthcare
[70]	IDS for IRSA	PCA	IRSA	DDoS	NSL_KDD	Environment

In view of the accessibility of combined highlights, the framework utilizes different covering based highlight choice strategies, from SVMs and choice trees to Guileless Bayes, to choose higher-request highlights, which are accumulated and falsely delivered. This model accomplishes a high acknowledgment exactness of up to 99.95% and is generally cutthroat with existing AI works for the equivalent dataset. Pundir et al.[66] have proposed a Malware identification strategy in IoT-empowered modern sight and sound climate with the assistance of AI approach MADP-IIME. MADP-IIME utilizes four kinds of AI methods to effectively distinguish the presence of malware assaults. MADP-IIME beats other related plans accomplishing 99.5% acknowledgment and 0.5% misleading positive rate. Security investigation showing the obstruction of the proposed MADP-IIME against different kinds of malware assaults. Anthi et al.[67] have proposed IDs model to adversary assaults can be utilized to target unaided classifiers by giving produced enemy DoS examples to a prepared model and figuring out their grouping conduct. An IoT network dataset containing both harmless and DoS parcels was utilized to choose, train, and test cutting edge reconnaissance classifiers with the J48 result. Hu et al.[68] have investigated an incomplete kernel based on attribute-free and multi-kernel k model data for IDS for 5G and IoT networks. Exploratory outcomes demonstrate the way that this technique can accomplish high-exactness bunching when test information is fragmented. It actually has a few restrictions in perusing execution and a few impediments while perusing a lot of information. Keserwani et al.[69] have proposed an IDS to recognize different assaults for IoT organizations. Dark wolf streamlining (GWO) and molecule swarm advancement (PSO) are utilized to separate significant IoT network attributes. To accomplish high assault discovery exactness, the gathered elements are taken care of to an Irregular Woods (RF) classifier. The GWO-PSO-RF NIDS model accomplished a normal precision of 99.66% for multi-class characterization. Duraisamy et al.[70] have proposed an assault recognition strategy in IoT shrewd urban communities utilizing MANFIS order. Information values taken by NSL_KDD dataset are utilized for preparing. The viability of this technique is tried by contrasting its exhibition and existing strategies. The CM-CSO applied in FS is thought about in contrast to the

current GA, HOA and Entropy-HOA, and the outcomes show that the proposed CM-CSO accomplishes the most noteworthy FV for all cycles. Then, at that point, MANFIS classifier is contrasted and existing SVM, ANN, DLNN and DLMNN as far as execution, awareness, exactness and F-measure. MANFIS acquires the most elevated upsides of these aspects for every hub. Table 5 sums up the examination holes gathered from cutting edge works connected with AI based IDS conspire for IoT.

4.6 Review on security attacks addressing using deep learning [71]-[80]

Li et al.[71] have proposed an IoT data highlight extraction and IDS depend on profound relocation learning model. Recreation results demonstrate the way that the proposed technique can ensure high identification rate and low bogus positive rate while further developing execution. As displayed in the trial segments, contrasted with the conventional techniques ELM and BP, the computation proposed in this paper has a higher chase efficiency and a more limited search time simultaneously. From distinguishing more assaults and mistake recognition rate, the productivity and viability of the proposed calculation are incredibly moved along. Almiani et al.[72] have presented a Artificial and fully automatic intrusion detection system to fog protection from cyber-attacks. The proposed multi-layer model of persistent neural networks is used to implement mist processing security close to end-clients and IoT gadgets. Nie et al.[73] have proposed a Information driven IDS by breaking down the connection load conduct of Side of the road Unit (RSU) in IoV against different assaults that cause irregular variances in rush hour gridlock stream. A profound learning system in view of Convolutional Brain Organization (CNN) is intended to catch the characteristics of connection load and detect intrusions targeting RSU. Sujanthi et al.[74] have proposed an addresses this issue by fostering a Solid Profound Learning (SecDL) approach for dynamic pack based WSN-IoT associations. To additionally foster energy viability, the organization is planned as a binary hexagon using mobile sink technology. Kunang et al.[75] have proposed Alternative solutions for profound learning compositional models through programmed hyper parameter enhancement consolidating lattice search and irregular hunt strategies. A mechanized hyper parameter advancement process decides hyper parameter values and optimal hyper parameter configuration to optimize detection performance.

Nie et al.[76] have proposed an IDS algorithm based on deep reinforcement learning follows traffic flow trends by extracting statistics from past network traffic for traffic prediction. Evaluations confirm the effectiveness of our algorithm in DDoS detection. Network traffic estimation is useful for various network management and security tasks. With 5G communication technology applications, network traffic exhibits more complex characteristics, which poses a great challenge to the network traffic estimation problem.

Tsogbaatar et al.[77] have presented a DeL-IoT is another profound outfit learning model-based system for IoT peculiarity recognition, which predominantly utilizes SDN to further develop discovery execution, switch-level powerful stream the board, short-and long haul gadget state estimation for anomalies, or dynamic SDN. Detect attacks. A deep and layered auto-encoder is proposed to extract layered features in a PNN training model to improve performance when solving the data stochastic problem. A method for dynamic flow management in the presence of attacks and device state estimation based on state tables. System managers can use these predictive features to proactively counter dynamic attacks from devices to physical infrastructure. Excellent performance on test bed and benchmark datasets with 99.8% and 99.9% recognition rates, respectively. Jothi et al.[78] have proposed a new adaptive deep learning model is the WILS framework. The presentation assessment of the proposed model is checked and contrasted and other learning models on various datasets, for example, constant dataset, CIDDC-001, UMSN15 and KDD dataset. Whale-optimized LSTM has demonstrated its accuracy, sensitivity, and superior performance compared to other algorithms in extracting malicious nodes in IoT networks and predicting various attacks on networks. Jithu et al.[79] have proposed a deep learning-based intrusion detection system for detecting IoT DDoS botnet assaults. The dataset utilized in this work was planned and created in a

virtual organization climate at the Digital Reach Lab at the UNSW Canberra Digital Center. The additional traffic information incorporates a mix of ordinary and assault traffic information. A significant level profound brain organization (DNN) was created for IoT networks that can recognize IoT botnet assaults. Fu et al.[80] have proposed a first trial on utilizing ill-disposed learning with CNN, LSTM and GRU in profound learning put together IDS in IoT climate with respect to interruption discovery dataset: CSE-CIC-IDS2018. To strengthen IDSs with various profound learning models and model strength using three adversary training methods to resist FGSM attacks. Table 6 illustrates a summary of research gaps collected from state-of-the-art works related to deep learning-based IDS scheme for IoT.

Table 6 Summary of research gaps with respect to deep learning based IDS scheme for IoT

Ref	Methodology	Feature extraction	DL technique	Attacks	Database	IoT application
[71]	IDS for smart city	PSO	Deep migration learning	Dos,Probing,R2l,URT	KDD CUP 99	Smart city
[72]	IDS for IoT	HBABO	FCM	U2R and R2L	NSL-KDD	Cloud
[73]	IDS for Iov	CNN	ITS	RSU, DDoS	TCP-SYN, UDP	Transportation
[74]	IDS for WSN-IoT	PSO	Co-Fit DNN	Implementation	ANFIS	Agriculture
[75]	IDS for HPO	DDQN	ML	Internal	NSL-KDD,AWID	Smart home
[76]	IDS for DRL	ImCNN	LEDEM	DDoS	CICDDoS2019	Smart Education
[77]	IDS for DeL-IoT	SVM	ANN	DDoS	Benchmark	Cloud
[78]	IDS for WILS-TRS	PSO	LSTM	DoS/DDOS	CIDDS-001, UNSWNB15, and KDD	Smart city
[79]	IDS for IoT Botnet	DNN	UNSW Canberra Cyber	DDoS Botnet	Darpa98, KDD99	Healthcare
[80]	IDS for Environments	PSO	Dynamic IDS, Anomaly detection	Buffer overflow	CSE-CIC-IDS2018	Agriculture

5. Results and Discussion

In this section, we describe the simulation results and perform a comparative analysis of various security issues and security methods for the IoT environment. Table 7 describes a comparative analysis of traditional IDS schemes [16]-[30] used as security mechanisms in IoT environments. Here, we measure the performance of state-of-the-art conventional IDS schemes using various quality metrics of detection rate and error rate. The recognition rate of the adaptive auto encoder [30] is very high 8.676%, 18.058%, 9.941%, 8.741%, 7.974%, 7.021%, 4.824%, 6.108% and 8.325%efficient than the other IDS schemes are SPN [31], Nonparametric Bayesian [32], SPN [33], IDS-CNN [34], SVM [35], one-class SVM [36], SVM [37], MKKM [38], and APAE [39], respectively. The error rate of adaptive auto encoder [30] is very low which is 42.72%, 24.841%, 33.743%, 37.935%, 24.499%, 28.006%, 45.262%, 26.489% and 40.525% efficient than other IDS schemes are SPN [31], Nonparametric Bayesian [32], SPN [33], IDS-CNN [34], SVM [35], one-class SVM [36], SVM [37], MKKM [38], and APAE [39], respectively. Fig. 5 shows the graphical representation of comparative analysis with respect to the different IDS schemes for IoT environment.

Table 7 Comparative analysis of traditional IDS schemes [31]- [40]

Ref	IDS scheme	Performance measures (%)	
		Detection rate	Error rate
[31]	SPN	87.561	24.356
[32]	Nonparametric Bayesian	78.565	18.562
[33]	SPN	86.348	21.056
[34]	IDS-CNN	87.498	22.478
[35]	SVM	88.234	18.478
[36]	one-class SVM	89.147	19.378
[37]	SVM	91.254	25.487
[38]	MKKM	90.023	18.978
[39]	APAE	87.897	23.457
[40]	Adaptive AE	95.879	13.951

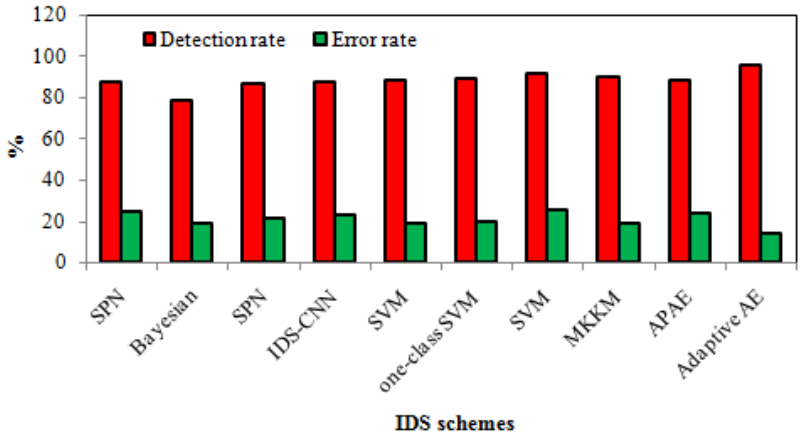

Fig. 5 Results comparison of traditional IDS schemes [31]-[40] used for IoT security solution

Table 8 describes the comparative analysis of different lightweight cryptography techniques [41]-[50] have used as the defense mechanism in IoT environment. Here, we validate the performance of state-of-arts lightweight cryptography techniques through the different quality measures are detection rate and error rate. The accuracy of BRISI lightweight crypto technique [50] is very high which is 5.756%, 4.525%, 3.118%, 3.434%, 2.237%, 1.547%, 2.198%, 1.547% and 2.525% higher than other lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively. The precision of BRISI lightweight crypto technique [50] is very high which is 7.877%, 6.428%, 5.767%, 6.097%, 4.93%, 3.786%, 3.084%, 1.955% and 0.833% higher than other lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively. The recall of BRISI lightweight crypto technique [50] is very high which is 9.765%, 8.966%, 7.533%, 4.368%, 7.23%, 5.695%, 3.614%, 3.298% and 1.321% higher than other lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively.

Table 8 Comparative analysis of lightweight crypto techniques [41]-[50]

Ref	Lightweight crypto schemes	Performance measures (%)						
		Accuracy	Precision	Recall	Specificity	F-measure	Detection rate	Error rate
[41]	LiKe	86.395	82.654	81.955	86.957	81.36549	76.354	25.394
[42]	LAM-CIoT	87.524	83.954	82.681	85.697	82.67542	77.687	26.574

[43]	Lightweight ECC	88.814	84.547	83.982	87.278	82.96358	78.981	26.873
[44]	LRBC	88.524	84.251	86.857	87.951	83.82547	79.687	27.982
[45]	S-box	89.621	85.298	84.257	88.951	84.3266	80.963	28.854
[46]	MCDM	90.254	86.324	85.652	88.967	84.69585	80.254	29.684
[47]	Lightweight ECC	89.657	86.954	87.542	89.671	85.32156	81.284	28.954
[48]	HashXor	90.254	87.967	87.829	90.761	89.65983	82.369	28.674
[49]	LMAAS-IoT	89.357	88.974	89.624	89.657	90.3266	81.857	29.654
[50]	BRISI	91.672	89.721	90.824	90.874	91.25848	83.412	21.056

The specificity of BRISI lightweight crypto technique [50] is very high which is 4.31%, 5.697%, 3.957%, 3.217%, 2.116%, 2.099%, 1.324%, 0.124% and 1.339% higher than other lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively. F-measure of BRISI lightweight crypto technique [50] is very high which is 10.841%, 9.405%, 9.089%, 8.145%, 7.596%, 7.191%, 6.506%, 1.752% and 1.021% higher than other lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively. The detection rate of BRISI lightweight crypto technique [50] is very high which is 8.676%, 18.058%, 9.941%, 8.741%, 7.974%, 7.021%, 4.824%, 6.108% and 8.325% efficient than the other lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively. The error rate of BRISI lightweight crypto technique [50] is very low which is 42.72%, 24.841%, 33.743%, 37.935%, 24.499%, 28.006%, 45.262%, 26.489% and 40.525% efficient than lightweight crypto techniques are LiKe [41], LAM-CIoT [42], Lightweight ECC [43], LRBC [44], S-box [45], MCDM [46], Lightweight ECC [47], HashXor [48] and LMAAS-IoT [49], respectively. Fig. 6 shows the graphical representation of comparative analysis with respect to the different lightweight cryptography techniques for IoT environment.

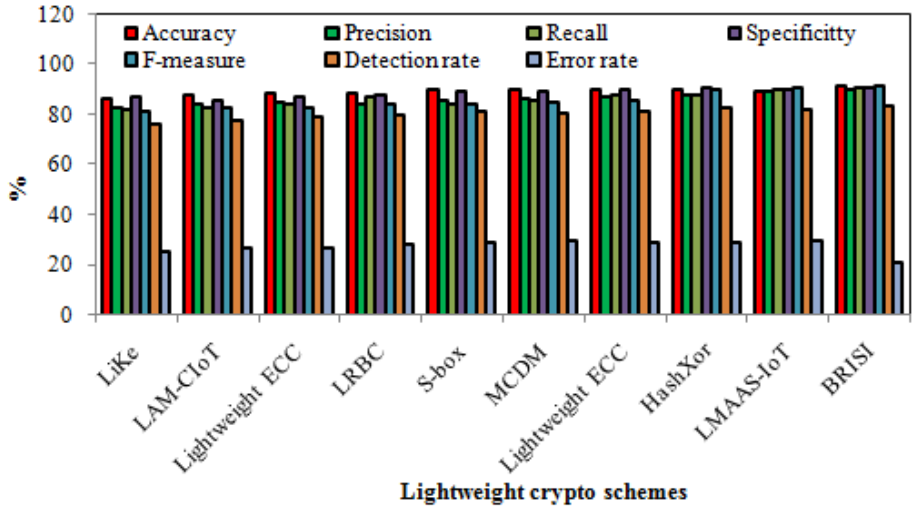

Fig. 6 Results comparison of lightweight cryptography techniques [41]-[50] for IoT environment

Table 9 Comparative analysis of blockchain based IDS schemes [51]-[60]

Ref	Blockchain based IDS	Performance measures (%)						
		Accuracy	Precision	Recall	Specificity	F-measure	Detection rate	Error rate
[51]	DNN, CNN Blockchain	86.29	83.36	82.36	81.36	78.69	79.36	25.54

[52]	Optimal blockchain	85.39	89.36	89.54	81.25	81.32	79.25	26.35
[53]	CA of multiple-PKI trust	89.23	87.36	83.26	82.54	82.96	78.45	23.65
[54]	SEA-Blockchain	90.58	91.89	87.96	89.54	83.96	79.45	28.94
[55]	Decentralized authentication Blockchain	86.86	82.54	81.23	84.63	83.54	78.45	28.65
[56]	Attack graph Blockchain	87.89	87.69	89.12	89.45	82.54	75.98	29.35
[57]	High level Petri nets	92.95	89.65	86.25	83.21	82.35	76.98	27.68
[58]	IBE-BCIOT	93.65	87.65	89.36	81.35	81.36	75.69	26.35
[59]	Blockchain with mapping	89.75	89.65	82.69	83.65	83.26	78.95	29.35
[60]	K-means cluster blockchain	94.36	94.235	91.235	89.56	89.104	85.457	18.748

Table 9 describes a comparative analysis of various blockchain-based IDS schemes [51]-[60] used as security mechanisms in IoT environments. Here we validate the performance of state-of-the-art blockchain-based IDS schemes through various quality measures. The accuracy of k-means clusters blockchain [60] is much higher, which is 8.552%, 9.506%, 5.437%, 4.006%, 7.948%, 6.857%, 1.494%, 0.752% and 4.88%. DNN, CNN Blockchain [51], Optimal Blockchain [52], Multi-PKI Trust CA [53], Sea-Blockchain [54], Decentralized Authentication Blockchain [55], Attack Graph Blockchain [56], Hi [56], High level Petri net [56]] 57], IBE-BCIOT [58] and mapping with blockchain [59] respectively. The precision of K-means clusters blockchain [60] is very high which is 711.54%, 5.173%, 7.296%, 2.488%, 12.41%, 6.945%, 4.865%, 6.988% and 4.865% higher than other blockchain based IDS schemes are DNN, CNN blockchain [51], optimal blockchain [52], CA of multiple-PKI trust [53], SEA-blockchain [54], decentralized authentication blockchain [55], attack graph blockchain [56], high level Petri nets [57], IBE-BCIOT [58], and blockchain with mapping [59], respectively. The recall of K-means clusters blockchain [60] is very high which is 9.728%, 1.858%, 8.741%, 3.59%, 10.966%, 2.318%, 5.464%, 2.055% and 9.366% higher than other blockchain based IDS schemes are DNN, CNN blockchain [51], optimal blockchain [52], CA of multiple-PKI trust [53], SEA-blockchain [54], decentralized authentication blockchain [55], attack graph blockchain [56], high level Petri nets [57], IBE-BCIOT [58], and blockchain with mapping [59], respectively. The specificity of K-means clusters blockchain [60] is very high which is 9.156%, 9.279%, 7.838%, 0.022%, 5.505%, 0.123%, 7.090%, 9.167% and 6.599% higher than other blockchain based IDS schemes are DNN, CNN blockchain [51], optimal blockchain [52], CA of multiple-PKI trust [53], SEA-blockchain [54], decentralized authentication blockchain [55], attack graph blockchain [56], high level Petri nets [57], IBE-BCIOT [58], and blockchain with mapping [59], respectively.

F-measure of K-means cluster blockchain [60] is very high which is 11.687%, 8.736%, 6.895%, 5.773%, 6.244%, 7.367%, 7.58%, 8.691% and 6.559% higher than other blockchain based IDS schemes are DNN, CNN blockchain [51], optimal blockchain [52], CA of multiple-PKI trust [53], SEA-blockchain [54], decentralized authentication blockchain [55], attack graph blockchain [56], high level Petri nets [57], IBE-BCIOT [58], and blockchain with mapping [59], respectively. The detection rate of K-means clusters blockchain [60] is very high which is 7.135%, 7.263%, 8.199%, 7.029%, 8.199%, 11.09%, 9.92%, 11.429% and 7.614% efficient than the other blockchain based IDS schemes are DNN, CNN blockchain [51], optimal blockchain [52], CA of multiple-PKI trust [53], SEA-blockchain [54], decentralized

authentication blockchain [55], attack graph blockchain [56], high level Petri nets [57], IBE-BCIOT [58], and blockchain with mapping [59], respectively. The error rate of K-means clusters blockchain [60] is very low which is 26.594%, 28.85%, 20.727%, 35.218%, 34.562%, 36.123%, 32.269%, 28.85% and 36.123% efficient than other blockchain based IDS schemes are DNN, CNN blockchain [51], optimal blockchain [52], CA of multiple-PKI trust [53], SEA-blockchain [54], decentralized authentication blockchain [55], attack graph blockchain [56], high level Petri nets [57], IBE-BCIOT [58], and blockchain with mapping [59], respectively. Fig. 7 shows the graphical representation of comparative analysis with respect to the different lightweight cryptography techniques for IoT environment.

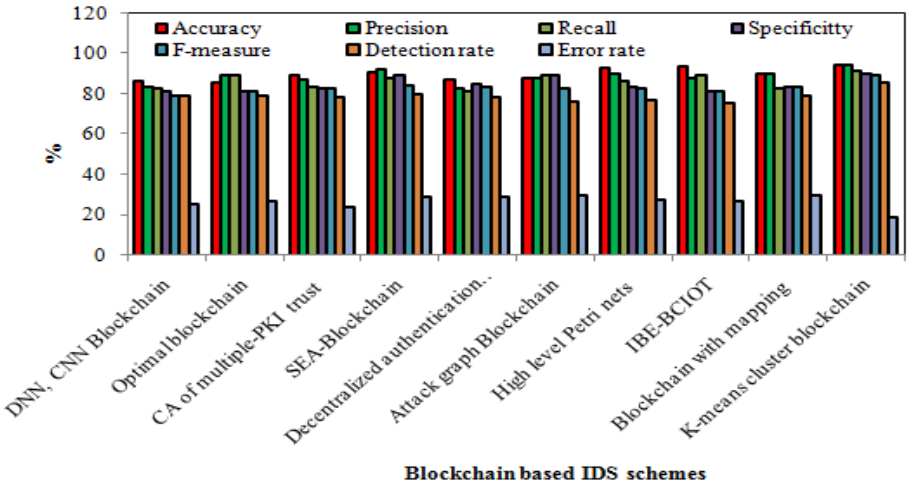

Fig. 7 Results comparison of blockchain based IDS schemes [51]-[60] for IoT environment

Table 10 describes a comparative analysis of various ML-based IDS schemes [61]-[70] used as security mechanisms in IoT environments. Here we validate the performance of state-of-the-art ML-based IDS schemes through various quality metrics. The accuracy of IRSA algorithm [70] is very high which is 6.543%, 6.235%, 5.337%, 5.071%, 4.698%, 3.631%, 2.676%, 1.432% and 2.897% higher than other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively. The precision of IRSA algorithm [70] is very high which is 7.255%, 5.57%, 5.694%, 4.572%, 3.474%, 5.126%, 2.692%, 1.212% and 5.67% higher than other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively. The recall of IRSA algorithm [70] is very high which is 9.343%, 7.446%, 7.051%, 5.847%, 5.94%, 4.338%, 4.015%, 3.402% and 2.22% 9higher than other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively. The specificity of IRSA algorithm [70] is very high which is 5.185%, 4.702%, 3.903%, 2.994%, 3.111%, 2.194%, 0.782%, 1.898% and 0.777% higher than other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively. F-measure of IRSA algorithm [70] is very high which is 6.877%, 5.695%, 6.088%, 5.291%, 5.407%, 3.055%, 3.091%, 4.214% and 2.347% higher than other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively. The detection rate of IRSA algorithm [70] is very high which is 6.783%, 5.901%, 5.028%, 3.763%, 3.749%, 2.539%, 5.803%, 1.764% and 2.25% efficient than the other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively.

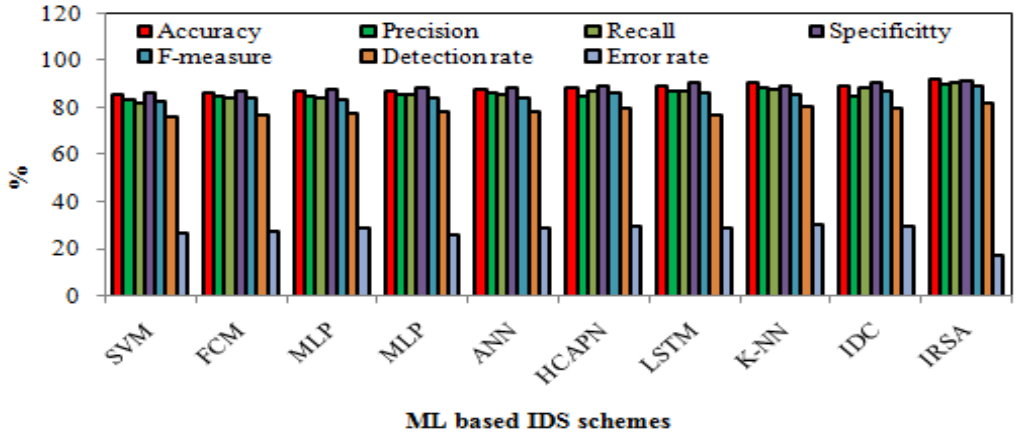

Fig. 8 Results comparison of ML based IDS schemes [61]- [70] for IoT environment

Table 10 Comparative analysis of ML based IDS schemes [61]-[70]

Ref	Blockchain based IDS	Performance measures (%)						
		Accuracy	Precision	Recall	Specificity	F-measure	Detection rate	Error rate
[61]	SVM	85.846	83.231	82.157	86.524	82.846	76.154	26.547
[62]	FCM	86.129	84.743	83.876	86.965	83.897	76.874	27.452
[63]	MLP	86.954	84.632	84.234	87.694	83.547	77.587	28.578
[64]	MLP	87.198	85.639	85.325	88.524	84.256	78.621	26.147
[65]	ANN	87.541	86.624	85.241	88.417	84.153	78.632	28.541
[66]	HCAPN	88.521	85.142	86.693	89.254	86.245	79.621	29.654
[67]	LSTM	89.398	87.326	86.985	90.542	86.214	76.954	28.635
[68]	K-NN	90.541	88.654	87.541	89.524	85.215	80.254	30.521
[69]	IDC	89.195	84.654	88.612	90.547	86.875	79.857	29.657
[70]	IRSA	91.856	89.742	90.624	91.256	88.963	81.695	17.562

The error rate of IRSA algorithm [70] is very low which is 33.846%, 36.027%, 38.547%, 32.834%, 38.467%, 40.777%, 38.669%, 42.459% and 40.783% efficient than other ML based IDS schemes are SVM [61], FCM [62], MLP [63], MLP [64], ANN [65], HCAPN [66], LSTM [67], K-NN [68], and IDC [69], respectively. Fig. 8 shows the graphical representation of comparative analysis with respect to the different ML based IDS schemes [61]- [70] for IoT environment.

Table 11 describes the comparative analysis of different DL based IDS schemes [71]- [80] have used as the defense mechanism in IoT environment. Here, we validate the performance of state-of-arts DL based IDS schemes through the different quality measures. The accuracy of CNNalgorithm [80] is very high which is 6.968%, 5.512%, 5.98%, 4.82%, 4.381%, 5.945%, 4.101%, 2.495% and 1.467% higher than other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively. The precision of CNN algorithm [80] is very high which is 8.119%, 7.274%, 7.255%, 6.103%, 5.325%, 4.781%, 4.006%, 3.196% and 2.451% higher than other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively. The recall of CNN algorithm [80] is very high which is 8.689%, 7.81%, 7.652%, 6.423%, 5.436%, 6.071%, 3.624%, 2.326% and 2.485% higher than other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively. The specificity of CNN algorithm [80] is very high which is 4.951%, 4.533%, 4.505%, 3.553%, 3.022%, 2.298%, 2.284%, 0.836% and 1.443% higher than other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively. F-measure of CNN algorithm [80] is

very high which is 8.808%, 7.858%, 7.688%, 7.355%, 6.203%, 5.939%, 4.215%, 3.1% and 1.988% higher than other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively.

Table 11 Comparative analysis of DL based IDS schemes [71]-[80]

Ref	Blockchain based IDS	Performance measures (%)						
		Accuracy	Precision	Recall	Specificity	F-measure	Detection rate	Error rate
[71]	Deep migration learning	84.523	82.456	81.235	86.145	81.841	76.954	25.314
[72]	FCM	85.846	83.214	82.017	86.524	82.694	76.123	26.547
[73]	Optimal CNN	85.421	83.231	82.157	86.549	82.846	76.154	26.157
[74]	Co-FitDNN	86.475	84.265	83.251	87.412	83.145	74.521	27.412
[75]	SVM-CNN	86.874	84.963	84.129	87.893	84.179	77.128	27.561
[76]	LEDEM	85.453	85.451	83.564	88.549	84.415	77.563	28.456
[77]	ANN	87.128	86.147	85.741	88.562	85.963	78.954	28.962
[78]	LSTM	88.587	86.874	86.896	89.874	86.963	79.856	29.874
[79]	DRNN	89.521	87.542	86.754	89.324	87.961	80.963	29.524
[80]	CNN	90.854	89.742	88.965	90.632	89.746	82.132	19.254

The detection rate of CNN algorithm [80] is very high which is 6.304%, 7.316%, 7.279%, 9.267%, 6.093%, 5.563%, 3.869%, 2.771% and 1.423% efficient than the other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively. The error rate of CNN algorithm [80] is very low which is 23.939%, 27.472%, 26.391%, 29.761%, 30.14%, 32.338%, 33.52%, 35.549% and 34.785% efficient than other DL based IDS schemes are Deep migration learning [71], FCM [72], Optimal CNN [73], Co-FitDNN [74], SVM-CNN [75], LEDEM [76], ANN [77], LSTM [78], and DRNN [79], respectively. Fig. 9 shows the graphical representation of comparative analysis with respect to the different DL based IDS schemes [71]-[80]for IoT environment.

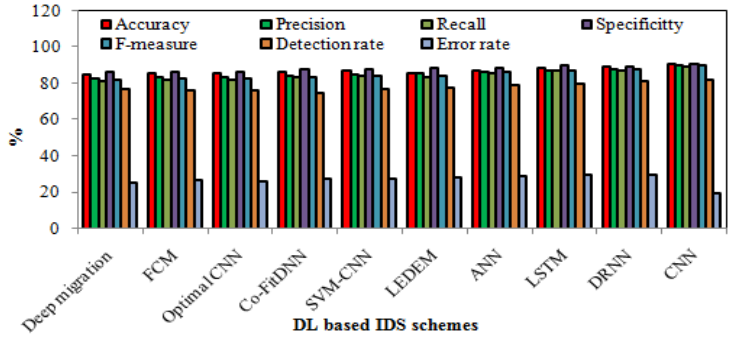

Fig. 9 Results comparison of DL based IDS schemes [61]-[70] for IoT environment

6. Conclusion

With the appearance of IoT, objects utilized in our regular routines can communicate with each other using the Internet. However, when using different technologies, several problems arise, among which the issue of security is important. To solve these problems, different cryptographic natives have been formulated. In any case, with the approach of quantum registering idea, these crypto graphics are not sufficiently solid. Hence, there is a need to foster cryptographic arrangements that give the normal degree of safety in post-quantum IoT organizations. In this work, we describe a new systematic review of security issues and security mechanisms in IoT environments. Several studies have recently been conducted proposing advanced security approaches for security solutions in IoT environments. Most of the research papers available in this area focus on the broad area of security measures in IoT environments. In this survey, we were able to collect about 80 research articles related to security measures in the IoT

environment for a systematic review. Our review includes open research challenges and future research directions. In addition, we discuss challenges and recommendations for developing various preventive care measures based on the findings of this study. With the rise of IoT, many security vulnerabilities have attracted the attention of the research community, from assaults on gadgets to assaults on information on the way. Likewise, the far reaching utilization of IoT in enterprises has made IoT a one of a kind field of examination. The tight coordination of the actual world with the virtual world using smart frameworks expands the gamble of modern IoT-based frameworks. So while studying IoT in this work

Our systematic literature review addresses the following research questions.

1. From brief systematic review of the literature, we conclude that there are several interventions in the context of IoT. With ever-increasing deployments and opportunities, an increasing number of attacks continue to exploit and compromise IoT devices. Malicious activities, DoS, DDoS, MITM and sweep attacks are the main types of attacks that can compromise IoT devices. The answer to RQ1 is that most IDS techniques applied to IoT environments rely primarily on IoT attacks, although they come from different sources.
2. However, with regards to RQ2, many of these methods are difficult to implement for various reasons. For example, it is important to ensure that attribute values used in detection differentiate between normal and abnormal traffic per network packet, with attribute values designed for network packet processing. This is a problem during extraction. Furthermore, when using a supervised learning method, it is necessary to acquire and/or generate labeled data. These difficulties can hinder the research and practical application of anomaly-based IDSs. Therefore, our research proposes an anomaly detection method that automatically extracts the feature without requiring specially labeled data for each use case.
3. For RQ3, we use encryption to protect network authentication, privacy, data integrity, and access control. However, due to the many limitations of IoT devices, traditional cryptographic protocols are no longer applicable to all IoT environments such as smart cities. As a result, researchers have proposed several lightweight cryptographic algorithms and protocols to protect data in IoT networks.
4. In response to RQ4, we combined multiple ML and DL technologies to provide a robust solution to address related security vulnerabilities and improve security for IoT environments. From our analysis, we can say that ML-based IDS techniques work well for specific attacks. However, they are not suitable for high traffic density. Therefore, our proposals and this study conclude that the accuracy of DL-based IDS techniques can be improved.
5. To address RQ5, we can analyze qualitative measures with respect to precision, accuracy, recall, F-measure, and specificity. Simulation results and comparative analysis show that SVM and CNN based IDS technique performs very effectively against security solutions for advanced security problems and IoT environments. In the future, we can further extend our research with the deep learning-based IDS schemes because all data and experimental support is available as open.

References

1. Asam, M., Khan, S.H., Akbar, A., Bibi, S., Jamal, T., Khan, A., Ghafoor, U. and Bhutta, M.R., 2022. IoT malware detection architecture using a novel channel boosted and squeezed CNN. *Scientific Reports*, *12*(1), pp.1-12.
2. Alawad, F. and Kraemer, F.A., 2022. Value of Information in Wireless Sensor Network Applications and the IoT: A Review. *IEEE Sensors Journal*.
3. Chen, Y., He, S., Wang, B., Duan, P., Zhang, B., Hong, Z. and Ping, Y., 2022. Cryptanalysis and Improvement of DeepPAR: Privacy-Preserving and Asynchronous Deep Learning for Industrial IoT. *IEEE Internet of Things Journal*.
4. Huang, C.Y., Chiang, Y.H. and Tsai, F., 2022. An Ontology Integrating the Open Standards of City Models and Internet of Things for Smart-City Applications. *IEEE Internet of Things Journal*, *9*(20), pp.20444-20457.
5. Zhou, X., Hu, Y., Wu, J., Liang, W., Ma, J. and Jin, Q., 2022. Distribution bias aware collaborative generative adversarial network for imbalanced

deep learning in industrial iot. *IEEE Transactions on Industrial Informatics*.

6. Chen, S., Xu, H., Liu, D., Hu, B. and Wang, H., 2014. A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), pp.349-359.
7. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. and Bangash, Y.A., 2020. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, *7*(10), pp.10250-10276.
8. Ferrag, M.A. and Shu, L., 2021. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet of Things Journal*, *8*(24), pp.17236-17260.
9. Nie, L., Sun, W., Wang, S., Ning, Z., Rodrigues, J.J., Wu, Y. and Li, S., 2021. Intrusion detection in green internet of things: a deep deterministic policy gradient-based algorithm. *IEEE Transactions on Green Communications and Networking*, *5*(2), pp.778-788.
10. Jahromi, A.N., Karimipour, H., Dehghantanha, A. and Choo, K.K.R., 2021. Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. *IEEE Internet of Things Journal*, *8*(17), pp.13712-13722.
11. Doshi, K., Yilmaz, Y. and Uludag, S., 2021. Timely detection and mitigation of stealthy DDoS attacks via IoT networks. *IEEE Transactions on Dependable and Secure Computing*, *18*(5), pp.2164-2176.
12. Zhang, Z., Deng, R., Yau, D.K. and Chen, P., 2021. Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid. *IEEE Internet of Things Journal*, *8*(8), pp.6608-6623.
13. Zhou, X., Liang, W., Li, W., Yan, K., Shimizu, S., Kevin, I. and Wang, K., 2021. Hierarchical adversarial attacks against graph neural network based IoT network intrusion detection system. *IEEE Internet of Things Journal*.
14. Zolanvari, M., Teixeira, M.A., Gupta, L., Khan, K.M. and Jain, R., 2019. Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), pp.6822-6834.
15. Ren, K., Zeng, Y., Cao, Z. and Zhang, Y., 2022. ID-RDRL: a deep reinforcement learning-based feature selection intrusion detection model. *Scientific Reports*, *12*(1), pp.1-18.
16. Chen, P.Y., Cheng, S.M. and Chen, K.C., 2014. Information fusion to defend intentional attack in internet of things. *IEEE Internet of Things Journal*, *1*(4), pp.337-348.
17. Zhang, K., Liang, X., Lu, R. and Shen, X., 2014. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, *1*(5), pp.372-383.
18. La, Q.D., Quek, T.Q., Lee, J., Jin, S. and Zhu, H., 2016. Deceptive attack and defense game in honeypot-enabled networks for the internet of things. *IEEE Internet of Things Journal*, *3*(6), pp.1025-1035.
19. Xu, T., Gao, D., Dong, P., Zhang, H., Foh, C.H. and Chao, H.C., 2017. Defending against new-flow attack in sdn-based internet of things. *IEEE Access*, *5*, pp.3431-3443.
20. Li, C., Qin, Z., Novak, E. and Li, Q., 2017. Securing SDN infrastructure of IoT–fog networks from MitM attacks. *IEEE Internet of Things Journal*, *4*(5), pp.1156-1164.
21. Yu, W. and Köse, S., 2017. A lightweight masked AES implementation for securing IoT against CPA attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *64*(11), pp.2934-2944.
22. Qiu, T., Liu, X., Han, M., Ning, H. and Wu, D.O., 2017. A secure time synchronization protocol against fake timestamps for large-scale internet of things. *IEEE Internet of Things Journal*, *4*(6), pp.1879-1889.
23. Zhang, P., Nagarajan, S.G. and Nevat, I., 2017. Secure location of things (SLOT): mitigating localization spoofing attacks in the Internet of Things. *IEEE Internet of Things Journal*, *4*(6), pp.2199-2206.
24. Lin, S.C., Wen, C.Y. and Sethares, W.A., 2017. Two-tier device-based authentication protocol against PUEA attacks for IoT applications. *IEEE Transactions on Signal and Information Processing over Networks*, *4*(1), pp.33-47.
25. Mangia, M., Pareschi, F., Rovatti, R. and Setti, G., 2017. Low-cost security of IoT sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks. *IEEE Transactions on Information Forensics and Security*, *13*(2), pp.327-340.

26. Tang, X., Ren, P. and Han, Z., 2018. Jamming mitigation via hierarchical security game for IoT communications. *IEEE Access*, *6*, pp.5766-5779.
27. Yin, D., Zhang, L. and Yang, K., 2018. A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access*, *6*, pp.24694-24705.
28. Xu, B., Wang, W., Hao, Q., Zhang, Z., Du, P., Xia, T., Li, H. and Wang, X., 2018. A security design for the detecting of buffer overflow attacks in IoT device. *IEEE Access*, *6*, pp.72862-72869.
29. Raoof, A., Matrawy, A. and Lung, C.H., 2018. Routing attacks and mitigation methods for RPL-based Internet of Things. *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1582-1606.
30. Wang, M., Xiao, D., Xiang, Y. and Wang, H., 2019. Privacy-aware controllable compressed data publishing against sparse estimation attack in IoT. *IEEE Internet of Things Journal*, *6*(4), pp.7305-7318.
31. Al-Hamadi, H., Chen, R., Wang, D.C. and Almashan, M., 2020. Attack and defense strategies for intrusion detection in autonomous distributed IoT systems. *IEEE Access*, *8*, pp.168994-169009.
32. Alhakami, W., ALharbi, A., Bourouis, S., Alroobaea, R. and Bouguila, N., 2019. Network anomaly intrusion detection using a nonparametric Bayesian approach and feature selection. *IEEE Access*, *7*, pp.52181-52190.
33. Wang, D.C., Chen, R. and Al-Hamadi, H., 2020. Reliability of Autonomous Internet of Things Systems with Intrusion Detection Attack-Defense Game Design. *IEEE Transactions on Reliability*, *70*(1), pp.188-199.
34. Abdollahi, A. and Fathi, M., 2020. An intrusion detection system on ping of death attacks in IoT networks. *Wireless Personal Communications*, *112*(4), pp.2057-2070.
35. Nimbalkar, P. and Kshirsagar, D., 2021. Feature selection for intrusion detection system in Internet-of-Things (IoT). *ICT Express*, *7*(2), pp.177-181.
36. Liu, J., Yang, D., Lian, M. and Li, M., 2021. Research on intrusion detection based on particle swarm optimization in IoT. *IEEE Access*, *9*, pp.38254-38268.
37. Kalnoor, G. and Gowrishankar, S., 2021. IoT-based smart environment using intelligent intrusion detection system. *Soft Computing*, *25*(17), pp.11573-11588.
38. Hu, N., Tian, Z., Lu, H., Du, X. and Guizani, M., 2021. A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *International Journal of Machine Learning and Cybernetics*, *12*(11), pp.3129-3144.
39. Basati, A. and Faghih, M.M., 2021. APAE: An IoT intrusion detection system using asymmetric parallel auto-encoder. *Neural Computing and Applications*, pp.1-21.
40. Siddiqui, A.J. and Boukerche, A., 2021. Adaptive ensembles of autoencoders for unsupervised IoT network intrusion detection. *Computing*, *103*(6), pp.1209-1232.
41. Tedeschi, P., Sciancalepore, S., Eliyan, A. and Di Pietro, R., 2019. LiKe: Lightweight certificateless key agreement for secure IoT communications. *IEEE Internet of Things Journal*, *7*(1), pp.621-638.
42. Wazid, M., Das, A.K., Bhat, V. and Vasilakos, A.V., 2020. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Applications*, *150*, p.102496.
43. Sadhukhan, D., Ray, S., Biswas, G.P., Khan, M.K. and Dasgupta, M., 2021. A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, *77*(2), pp.1114-1151.
44. Biswas, A., Majumdar, A., Nath, S., Dutta, A. and Baishnab, K.L., 2020. LRBC: a lightweight block cipher design for resource constrained IoT devices. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-15.
45. Rashidi, B., 2021. Compact and efficient structure of 8-bit S-box for lightweight cryptography. *Integration*, *76*, pp.172-182.
46. Ning, L., Ali, Y., Ke, H., Nazir, S. and Huanli, Z., 2020. A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for internet of health things. *IEEE Access*, *8*, pp.220165-220187.
47. Hammi, B., Fayad, A., Khatoun, R., Zeadally, S. and Begriche, Y., 2020. A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal*, *14*(3), pp.3440-3450.

48. Choudhury, H., 2021. HashXor: A lightweight scheme for identity privacy of IoT devices in 5G mobile network. *Computer Networks*, *186*, p.107753.
49. Alsahlani, A.Y.F. and Popa, A., 2021. LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. *Journal of Network and Computer Applications*, *192*, p.103177.
50. VG, K.K., 2021. Design and implementation of novel BRISI lightweight cipher for resource constrained devices. *Microprocessors and Microsystems*, *84*, p.104267.
51. Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F. and Guizani, M., 2019. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, *7*, pp.18611-18621.
52. Yohan, A. and Lo, N.W., 2020. FOTB: a secure blockchain-based firmware update framework for IoT environment. *International Journal of Information Security*, *19*(3), pp.257-278.
53. Ren, Y., Zhu, F., Zhu, K., Sharma, P.K. and Wang, J., 2021. Blockchain-based trust establishment mechanism in the internet of multimedia things. *Multimedia Tools and Applications*, *80*(20), pp.30653-30676.
54. Shi, N., Tan, L., Yang, C., He, C., Xu, J., Lu, Y. and Xu, H., 2021. BacS: a blockchain-based access control scheme in distributed internet of things. *Peer-to-peer networking and applications*, *14*(5), pp.2585-2599.
55. Khalid, U., Asim, M., Baker, T., Hung, P.C., Tariq, M.A. and Rafferty, L., 2020. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, *23*(3), pp.2067-2087.
56. Sahay, R., Geethakumari, G. and Mitra, B., 2020. A novel blockchain based framework to secure IoT-LLNs against routing attacks. *Computing*, *102*(11), pp.2445-2470.
57. Hameed, K., Garg, S., Amin, M.B. and Kang, B., 2021. A formally verified blockchain-based decentralised authentication scheme for the internet of things. *The Journal of Supercomputing*, *77*(12), pp.14461-14501.\
58. Shao, S., Chen, F., Xiao, X., Gu, W., Lu, Y., Wang, S., Tang, W., Liu, S., Wu, F., He, J. and Ji, Y., 2021. IBE-BCIOT: An IBE based cross-chain communication mechanism of blockchain in IoT. *World Wide Web*, *24*(5), pp.1665-1690.
59. Ammi, M., Alarabi, S. and Benkhelifa, E., 2021. Customized blockchain-based architecture for secure smart home for lightweight IoT. *Information Processing & Management*, *58*(3), p.102482.
60. Hossein, K.M., Esmaeili, M.E., Dargahi, T., Khonsari, A. and Conti, M., 2021. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Computer Communications*, *180*, pp.31-47.
61. Liu, L., Xu, B., Zhang, X. and Wu, X., 2018. An intrusion detection method for internet of things based on suppressed fuzzy clustering. *EURASIP Journal on Wireless Communications and Networking*, *2018*(1), pp.1-7.
62. Verma, A. and Ranga, V., 2020. Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, *111*(4), pp.2287-2310.
63. Rahman, M.A., Asyhari, A.T., Leong, L.S., Satrya, G.B., Tao, M.H. and Zolkipli, M.F., 2020. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustainable Cities and Society*, *61*, p.102324.
64. Atul, D.J., Kamalraj, R., Ramesh, G., Sankaran, K.S., Sharma, S. and Khasim, S., 2021. A machine learning based IoT for providing an intrusion detection system for security. *Microprocessors and Microsystems*, *82*, p.103741.
65. Rahman, M.A., Asyhari, A.T., Wen, O.W., Ajra, H., Ahmed, Y. and Anwar, F., 2021. Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection. *Multimedia Tools and Applications*, *80*(20), pp.31381-31399.
66. Pundir, S., Obaidat, M.S., Wazid, M., Das, A.K., Singh, D.P. and Rodrigues, J.J., 2021. MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach. *Multimedia Systems*, pp.1-13.
67. Anthi, E., Williams, L., Javed, A. and Burnap, P., 2021. Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. *computers& security*, *108*, p.102352.

68. Hu, N., Tian, Z., Lu, H., Du, X. and Guizani, M., 2021. A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *International Journal of Machine Learning and Cybernetics*, *12*(11), pp.3129-3144.
69. Keserwani, P.K., Govil, M.C., Pilli, E.S. and Govil, P., 2021. A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. *Journal of Reliable Intelligent Environments*, *7*(1), pp.3-21.
70. Duraisamy, A. and Subramaniam, M., 2021. Attack Detection on IoT Based Smart Cities using IDS Based MANFIS Classifier and Secure Data Transmission Using IRSA Encryption. *Wireless Personal Communications*, *119*(2), pp.1913-1934.
71. Li, D., Deng, L., Lee, M. and Wang, H., 2019. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *International journal of information management*, *49*, pp.533-545.
72. Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S. and Razaque, A., 2020. Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, *101*, p.102031.
73. Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J. and Li, Y., 2020. Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. *IEEE Transactions on Network Science and Engineering*, *7*(4), pp.2219-2230.
74. Sujanthi, S. and NithyaKalyani, S., 2020. SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT. *Wireless Personal Communications*, *114*(3), pp.2135-2169.
75. Kunang, Y.N., Nurmaini, S., Stiawan, D. and Suprapto, B.Y., 2021. Attack classification of an intrusion detection system using deep learning and hyper parameter optimization. *Journal of Information Security and Applications*, *58*, p.102804.
76. Nie, L., Sun, W., Wang, S., Ning, Z., Rodrigues, J.J., Wu, Y. and Li, S., 2021. Intrusion detection in green internet of things: a deep deterministic policy gradient-based algorithm. *IEEE Transactions on Green Communications and Networking*, *5*(2), pp.778-788.
77. Tsogbaatar, E., Bhuyan, M.H., Taenaka, Y., Fall, D., Gonchigsumlaa, K., Elmroth, E. and Kadobayashi, Y., 2021. DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT. *Internet of Things*, *14*, p.100391.
78. Jothi, B. and Pushpalatha, M., 2021. WILS-TRS—A novel optimized deep learning based intrusion detection framework for IoT networks. *Personal and Ubiquitous Computing*, pp.1-17.
79. Shareena, J., Ramdas, A. and AP, H., 2021. Intrusion detection system for iot botnet attacks using deep learning. *SN Computer Science*, *2*(3), pp.1-8.
80. Fu, X., Zhou, N., Jiao, L., Li, H. and Zhang, J., 2021. The robust deep learning–based schemes for intrusion detection in Internet of Things environments. *Annals of Telecommunications*, *76*(5), pp.273-285