Chapter 3
IoT Data Security with Machine Learning Blckchain: Risks and Countermeasures



Koustav Kumar Mondal and Deepsubhra Guha Roy

3.1 Introduction

We have seen industries change from producing only goods to developing a grid of products acknowledged as the Internet-of-Things (IoT) and finally generating a smart product grid that offers a range of irreplaceable connected services [1, 2]. As per Aksu et al. [3], every three minutes, two devices are linked to the Internet. An growing amount of network traffic has resulted from this connectivity besides the exponential development of IoT devices. Challenges such as protection and confidentiality of operator data and substantiation and confirmation of strategies have emerged due to this connectivity [4]. In 2013, for instance, hackers compromised one billion yahoo accounts [5]. One hundred and forty-six million customers of eBay were underneath outbreak in 2014[6]. In 2017, one hundred and forty-four million Equifax clienteles had their private details compromised, continuing the growing pattern of attacks. Likewise, as noted in [7], their eight hundred and twenty thousand consumer accounts were abused by a five billion dollar toy industry in 2017. Over two and half million soundtracks, of which a limited were kept for payoff, were also included. Cybersecurity disasters are full of recent cyber history, from major data breaks to safekeeping vulnerabilities in billions of computer chip and lockdowns of computer grids before a imbursement has been made [8]. IoT devices have a multitude of protection and privacy problems that are growing every day. Security and privacy are therefore major challenges in dynamic and source-inhibited IoT surroundings and essential to be addressed efficiently. As the attacks become

K. K. Mondal
School of Computational Science, Department of IT, Maulana Abul Kalam Azad University of Technology, WB, Simhat, Haringhata, Nadia, Kolkata, West Bengal 741249, India

D. Guha Roy (✉)
Mobile and Cloud Lab, Institute of Computer Science, University of Tartu, Ulikooli 17–324, 50090 Tartu, Estonia
e-mail: roysubhraguha@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

A. Makkar and N. Kumar, *Deep Learning for Security and Privacy Preservation in IoT*, Signals and Communication Technology,
https://doi.org/10.1007/978-981-16-6186-0_3

sophisticated day by day, the security problems in the IoT are rising. Milosevic et al. [9] emphasized that influential computation policies, such as desktop computational devices, could be gifted to use specialised tools to detect malware. IoT systems have limited resources, however. Similarly, conventional cybersecurity frameworks and applications are not sufficiently effective to identify minor variations in attacks or zero-day outbreaks [10], meanwhile individually essential to be periodically modified. In addition, the changes are not accessible in real-time by the provider, rendering the network vulnerable. Algorithms for ML can be cast-off to progress the IoT setup (such as nifty devices and IoT entries) [11], as well as to improve the efficiency of cybersecurity systems. These procedures can analyse grid circulation, update danger information records, and retain the fundamental networks safe from novel outbreaks, based on existing knowledge of cyber threats [12]. In addition to using ML algorithms, researchers have also begun to secure the underlying structures with the groundbreaking Blockchain (BC) technique [9, 13–17]. Even though ML procedures and BC approaches have been technologically advanced to contract with IoT virtual terrorizations, compounding these deuce is somewhat new that desires to be investigated. Confidentiality drives with security hand in hand. Price et al. described confidentiality as a collection of rules based on the application [18]. The authors clarify that the instructions for in what way the data can stream be subject to on the people elaborate, procedures, regularity, and reasons for accessing the data. There are several applications that include security and privacy protection for personal information, such as wearable devices [3], Vehicular Area Network (VANET), healthcare, and smart-home [19, 20], for example. For example, the network is based on the data collected from devices in a crowdsensing application such as VANET to make smart decisions on the current traffic conditions. However, due to insufficient privacy-preserving measures and related risks, computer users may be reluctant to participate. In recent years, comprehensive studies focused on ML procedures and BC procedures [9, 12–17] have been carried out to secure system data and maintain the privacy of users.

3.2 Challenges in IoT

Internet-of-Things mentions to a huge amount of varied perception instruments, either on a LAN or over the Internet, communicating with each other [21]. Owing to the obtainable possessions of end strategies, IoT risks vary greatly from traditional networks [2]. IoT devices have limited memory and processing capacity, while powerful servers and computers with ample resources are part of the traditional Internet. Because of this, multifactor security layers and complex protocols will protect a conventional network, which is what can not be afforded by a real-time IoT device. IoT systems utilise fewer protected radiocommunication networking broadcasting, such as LoRa, ZigBee, 802.15.4, and 802.11a/b/n/g/p., as opposed toward conventional networks. Finally, IoT devices have distinct data contents and formats

owing to application-precise features and absence of mutual OS, construction it difficult to establish a standard safety protocol [22]. Both of these drawbacks variety IoT vulnerable to various threats to safety and confidentiality, thereby initial places for different categories of outbreaks. In a network, the likelihood of an outbreak intensifications with the scale of the grid. The IoT grid therefore takes additional flaws than a conventional grid, such as a corporation workplace, for instance.

Furthermore, usually multi-vendor devices with various specifications and protocols are IoT devices that communicate with each other. It is a challenge to communicate between such devices that needs a trusted third party to serve as a bridge [23]. In addition, many reports have posed questions about software updates to billions of smart devices on a daily basis [15, 24]. An IoT device's computing resources are partial, thus the abilities of addressing forward-thinking terrorizations are besmirched. IoT susceptibilities could be situated secret as unique and general, to summarise. For instance, IoT devices are unique to vulnerabilities such as battery-drainage attack, standardisation, and lack of confidence, and Cyberspace-congenital exposures can be considered as communal susceptibilities. In the past [25], numerous IoT intimidations and their categorisation take be situated familiarized. We address the most common IoT threats identified in the historical period and try to categorize them hooked on categories of protection and confidentiality.

3.2.1 Security Threats

The elementary principles of protection and confidentiality orbit everywhere the CIA triumvirate of Data Concealment, Information Truthfulness, and Grid Approachability [26]. In IoT, information can be whatever, such as the identity information of a user, Wrappers submitted to a server side from a security camera, a key-fob facility provided by a operator to his vehicle, or a multimedia conversation between two individuals. Any unauthorised disclosure of information will result in either confidentiality, honesty, or availability being violated. When a threat affects confidentiality, it is a threat to privacy. Both data integrity and network stability are affected by security threats.

3.2.1.1 Denial of Service

Of all security threats, Denial of Service (DoS) has the most simple implementation in contrast. In addition, an ever rising number of malfunctioning IoT devices has made DOS an intruder favourite weapon. The main aim of a DoS outbreak is to consume invalid requests into the network refers to network capabilities, such as bandwidth ingesting, being drained. As a result, the facilities are not real Oh accessible. Users. Users. Distributed DoS (DDoS) is an enhanced DoS attack version where a single target is attacking multiple outlets, making detecting and stopping attacks even more challenging. [27, 28]. While various kinds of DDoS occurrences exist, they have

all the same goal. SYN overflowing [29] (where an invader directs successive SYN applications to a target), Internet Control Message Protocol (ICMP) outbreaks [28] (a lot of ICMP packets are sent in the spoofed IP of the suspect.), conflict outbreaks [30] (using a comprehensive and dynamic botnet execution) and User Datagram Protocol (UDP) flooding are just a few variants of DDoS attacks. Botnet Attack [31] is a type of IoT network DDoS attack. The botnet is a group of Iot systems (sensors), which are conflict to strike a specific target for instance, a banking database. Malicious software intrusion can be carried out on a variety of protocols such as MQTT, DNS and Hypertext Transfer Protocol (HTTP), as specified in [31]. This is not the only solution. In the IoT setting, multiple methods are proposed for preventing DoS. Diro et al. [32] was using the auto-learning capabilities of Neural Network (DL) approaches to diagnose a threat in the fog-to-things climate. Abeshu et al. [27] recommended regulation of the DDoS outbreak by using dispersed DL on mist computation in another report. Tan et al. Intrusion Detection Method (IDS) is a series of research efforts using current ML and DL algorithms to mitigate DDoS attacks. Sharma et al. and Tselois et al. piercing obtainable, respectively, the problems of Software-Defined-Networks (SDN) flooding. The training emphasized that due to the absence of validation in the unadorned-text TCP station, the SDN's top layer was vulnerable to visceral power outbreaks.

3.2.1.2 Man-In-The-Middle Attack

MiTM was just one of a virtual world's oldest threats [33]. It is possible to categorise spoofing and impersonation as MiTM assaults. A node X intended to communicate with destination B, for example, the intruder MiTM who is trying to impersonate direction B may interact. Likewise, an intruder might use an Authenticated link, but the aim on the unsecured HTTP connection, to be able to load assaults on the database on Authentication striping. Recently, several studies have centered on enhancing MiTM defense [3, 23, 34]. Ahmad et al. [35] explored a medical situation in which a persevering gets a dose of insulin immediately. This program is vulnerable to lethal internal threats. For starters, Tang et al. effectively exposing the flow of users to Attackers in the wireless network repositories for smartphone applications; Similarly, Chatterjee et al. [36] highlighted current authentication methods in wireless mobile devices using a hidden key, in line with the impersonation attacks. This key was saved and used for digital signatures or hash-based encryption in non-volatile memory. Aside from being vulnerable, power was inefficient in this technique. Similarly, OAuth 2.0, the most recent and commonly used IoT protocol, suffers from attacks by Cross-site regeneration falsification (CSRF). The OAuth Mechanism is a time—intensive procedure which authenticates devices manually. The physical-layer security weakness in wireless authentication was stated in another study by Wang et al. They argued that, particularly in dynamic networks, the latest radio channel knowledge correlation analysis is frequently inaccessible with systems to compare the Alice channel history to detect the Eve spotter on Wi-Fi communication.

3.2.1.3 Malware

Virus is a malicious malware abbreviated form. The number of IoT devices has grown over the last few years, along with regular IoT package updates, where an intruder may use to send spam on a device and conduct fraudulent behaviors. Malicious software is widely considered to occur as a malware, spyware, worm, cheval, rootkit or malvertising [37]. A few examples that could be affected are smart home appliances, healthcare equipment, and vehicular sensors. On the Battlefield Stuff (IoBT) Internet, Azmoodeh et al. [38] studied malware. Usually, such offenders are effectively and highly qualified state-sponsored. Aonzo et al. [12], Feng et al. [39], and Wei et al. endeavored to practice various supervised ML algorithms to protect resource-constrained android devices from malware attacks. The trainings in [15, 40] as long as a thorough review of the recognition of malware and emphasized a range of safety escapes on the Android display place, in specific, on the intra application form application layer.

3.2.2 Privacy Threats

Iot nodes and their information are, in addition to safety risks, susceptible to assaults on anonymity, such as sniffing, deanonymization and assumption attacks. And if records are in motion or sleeping, the effect is on data safety. In this chapter, we deal with multiple privacy threats.

3.2.2.1 MiTM

We assume that it is possible to classify MiTM attacks into Active MiTM Attacks (AMA). MiTM Attacks (PMA) and Passive. Data transfer between two devices is passively listened to by the PMA. While privacy is violated by the PMA, they do not modify the data. An intruder who has admittance to a computer will Spot quietly for months prior to endeavoring an assault. With the rise in the number of cameras in IoT, devices such as the impact of PMA, the wake-up and the sniffing, including dolls, smartphones and wristwatches are high. The AMA however has a heavy impact on the manipulation of data. Acquired either by engaging with a consumer who pretends to be someone else, such as impersonation, For instance, authorization attack, or accessing a profile without consent.

3.2.2.2 Data Privacy

Data confidentiality attacks may be categorized as Aggressive, MiTM outbreaks, ADPA in addition Passive Data confidentiality attacks (PDPA). Data security is associated to database theft, data misuse, identity stealing and re-identification [41].

Re-identification occurrences are similarly acknowledged as inferenz outbreaks also are constructed on de-anonymisation, location recognition and aggregation of knowledge [41]. The key goal of these attacks is to gather data from different sources and to identify targets. Data from different sources. Any attackers may use the collected data to personify a particular objective. Any attack that changes information, for instance data theft, can be categorized as ADPA, while re-identification and statistics outflow are cases of PDPA.

3.3 Existing Review Papers Using ML Algorithms as a Solution

With emerging technologies, drudges are becoming advanced, making conventional attack-prevention approaches cumbersome. For a resource-constraint IoT system, protection becomes more challenging. One of the commonly used methods is ML algorithms to assist in detecting these attacks. Based on that acquired knowledge, ML could be specified as a capacity for data capability and the adjustment of ML model performance [21]. ML allows robots wise enough through learning from previous results and enhancing them to achieve more results. Many Quantitative methods have proved incredibly helpful in minimizing security and privacy risks. In the subsequent sections, we analyse these tactics in profundity.

3.3.1 Security Efforts

The programme has enhanced information exchange and interacting schemes beyond the Cyberspace. We now possess state-of-the-art, configurable software-based machines denominated Software Defined Network (SDN) that can be configured to suit a client's requirements. Cutting-edge this case, using the ML algorithms, Restuccia et al. [42] endeavored to exhibit the taxonomy of contemporary IoT preservation intimidations in addition their resolutions in SDN. They also suggested dividing the data acquisition manner into three planes, specifically IoT validation, IoT transatlantic networking, and IoT information collection & validation. An IoT system's main task is to collect data from IoT devices. The inquiry bestowed a concise summary of ML algorithms utilized to alleviate protection drives, such as distinguishing cross-layer ill-disposed strikes, using Bayesian learning, furthermore using neural networks to estimate information efficacy. The report, however, requires an in-depth knowledge of the base of the algorithms of the ML. Sharmeen et al. [43] intended to support application designers in the sustained use of Application Program Interfaces (APIs) throughout the growth of Industrial IoT mesh applications. The authors proposed that the ML example could be equipped to distinguish malware by using three varieties of latent, effective, and heterogeneous narratives.

Precise dissection of individual peculiarity type is implemented using production metrics of a dataset, wrenching peculiarity methodology, characteristic determination criteria, efficiency, and discovery process. Versatile discovery arrangements were assessed for a particular specialty set, but RF, SVM, KNN, J48, and NB are universally used. Sharmeen et al. [43] settled that variegated interpretation rendered versatility in selecting latent and changing aspects to enhance recognition process certainty. However, this article is restricted to one (android device) application and one (malware) safeguard fulmination. Between 2015 and 2018, Costa et al. [44] selected papers and affirmed that neither task contributed an in-depth appearance of the utilization of ML in every sense of apprehension of IoT transgression. The research To enhance IoT security, the state-of-the-art, as well as outmoded ML-based procedures, were checked. The most extensively utilized datasets and methodologies utilized in writing correlated to IoT protection were also discussed. However, the paper has not checked the current security or privacy risks from the IoT.

Similarly, Chaabouni et al. [10] including focused toward the apprehension systems for IoT-based channel intervention. The authors posed IoT construction and layer-wise occurrences and confidential by zones (opinion panel, chain layer, and application tier) and sketch provocations (before-mentioned as heterogeneity, versatility, reliance, and isolation, supply detentions, accessibility, and partaking of data). Some traditional IoT safety tools were obtained, including those investigating IoT regularities' Irregularity and Hybrid Network IDS (ANIDS). A thorough identification of standard NIDS was given for IoT operations treatment, apprehension methodologies, and innovative consequences. Moreover, the investigation explained whereby the IoT learning-based NIDS could determine the trials fronted through their traditional IoT commensurate systems. Finally, with an emphasis on ML algorithms, top IoT NIDS proposals were compared.

3.3.2 Privacy Efforts

Machine Learning obtains some immature data useful information, while solitude remains shielded by data concealment [45]. There are three modules in the ML method, according to Al-Rubaie et al. [41]: I information, (ii) estimate, and (iii) producing. This comparison moreover argued that solely if an indivisible personality dominated every three modules could isolation be shielded. Now, billions of IoT projects such as smartphones, wellness tracking sensors, and activity cameras, including temperature sensors, gather data worldwide, so one single-ownership situation can not be affirmed. As mentioned earlier, the problem sparked researchers' enthusiasm to propose new and improved ML algorithms that protect privacy. For instance, Zhang et al. raised the lack of privacy security mechanisms in a VANET setting. Vehicle nodes in VANET prefer to collaboratively learn, raising questions about privacy, anywhere each wicked junction may access confidential data through assuming of these data observed. They have restricted computation and memory for a single node Capabilities. Managing collaborative Characters among dispersed

ML algorithms plus addressing privacy problems, the solution was proposed by suggesting effective differential concealment principles to preserve an instruction dataset's secrecy. Transportation supervision arrangements for people, including healthcare pieces of equipment, remain pair of several standard IoT sensing technologies that necessitate perpetual development. Every robust, valuable data for the before-mentioned applications is reached immediately by Mobile Crowd-Sensing (MCS) from users. Xiao et al. checked the isolation risks associated with MCS, collecting these details of the concern and uploading the participants to the MCS server sensing reports of their climate. This exchange of information poses severe risks to the associates and the MCS server concerning sequestration. The system is vulnerable to privacy leakage, fake sensing strikes (addressing fraudulent statements to each server to limit sensing strains), including forwarding persistent fulminations (creating seclusion leakage aloft any lengthened term). This system is prone to privacy leakage. Furthermore, the survey suggested privacy protection for the DNN and CNN and counter-measurement of false sensing for the DBN, including DQN. The review was, however, limited to one application (MCS) only.

3.4 Existing Review Papers Using Blockchain as a Solution

The technology behind this notorious crypto-currency is Blockchain, frequently mistaken by some as a synonym for Bitcoin. It is a distributed ledger stored in blocks with the data. These wedges are in direction and connected to individually, creating one concatenation cryptographically into a process that performs this difficult to transform some data toward a distinct segment computationally [46]. This framework allows concerning immutation, decentralization, a threshold of faults, accountability, verification, auditability and confidence [32, 45]. There is neither a unique consensus on every BC form, although they are often unrestricted, individual, including consortium. Unrestricted rather permission-less BC is convenient to everyone to be accessed by anyone [47]. Individual/authorized blockchains, on appropriate other guidance, individual/sanctioned blockchains are performed by one or more, so not all can obtain them. The transactions here are quicker; only a few chosen can acquire a performance, thereby achieving a unison. To highlight BC techniques' importance, many reflections and critique expositions [22, 24, 31, 32, 37, 45, 48–50] have been published and may remain each valuable authorization toward these occupied in reading added wherein BC into depth. The latest research inspections approaching managing IoT protection, including isolation using BC schemes, are reviewed in this section.

3.4.1 Security Efforts

For all cases of IoT use, protection has been the prime subject of concern. Lots of things to address security problems in the IoT domain, work focused on BC techniques has emerged. Banerjee et al. [51] presented a report on IoT protection, characterized by safety procedures such as trespass apprehension and restraint regularity (IDPS), cooperative protection, including the ominous token. In addition, IDPS is defined by techniques, chain construction, including utilization. Collaborative safety furthermore auspicious protection exist addressed in-depth after that. Collaborative protection methods are categorized in the same study by network architectures and applications.

Security concerns associated with key superintendence, path administration, and corporation superintendence in IoT continue to be addressed in another study by Khan et al. [52, 52] classified those preservation intimidations toward IoT panels, including their explications based on BC. Low-level intermediate-level, and high-level security problems were categorised as IoT security issues. Khan et al. [52] assume that the low-level safety problems are squeezing foes, precarious initialization, parodying, fragile environmental interface, including slumber divestment initiatives. Micro intermediate-level preservation concerns are reiteration, RPL routing strikes, sinkhole, Sybil assault approaching amid layers, transport-level end-to-end sanctuary, assembly substantiation, including authentication. Insecure interfaces, CoAP Internet protection, insecure applications, and middleware security are high-level security concerns. The analysis then produced a thorough mapping of the preceding issues among those IoT architecture zones that affected various of them amidst suggested clarifications. Toward every point, the writers explored whereby some of the most important IoT security issues could be resolved and solved using BC techniques. This study highlighted the preservation uncertainties associated with an individual panel of IoT nevertheless failed to address the provision of BC-based explications to certain preservation fulminations.

Furthermore, Reyna et al. studied in [17] whence BC methods in the IoT could theoretically boost protection (data reliability). Since the whole concerning the summonses for BC procedures, each study listed security threats. Most attacks, double-spend attacks, and DoS attacks were the security threats identified in the report. The research also highlights the integration of BC methods, BC utilization, and BC principles with IoT. However, this research created not embrace many distinct IoT-related safeguard assaults, which was a drawback of this survey.

On the other hand, during extension to preservation issues, fresh advances within IoT, including BC integration, Panarello et al. [53] comprehensively analysed BC consensus protocols. The past literature was classified based on domain measures, accompanied by a comprehensive outline regarding specific contemporary BC-based solutions.

Kumar et al. [54] provided a concise summary regarding IoT security problems, including difficulties, before-mentioned as False authentication including Spoofing. Tamper-proof data, conferred, dynamic information, robustness, and assigned and

authorized information distribution are some of BC's benefits for large-scale IoT systems. They were following that the review presented the request wise BC founded IoT provocations. The authors of [55] emphasized IoT preservation problems furthermore presented their solutions based on BC. That thought preeminent highlighted specific criteria for IoT safeguard and its hurdles under six separate operation fields, such as intelligent cities, healthcare, intelligent networks, transportation, intelligent houses, furthermore development. The writers addressed the taxonomy of IoT preservation explications before-mentioned, as confidentiality was also prepared comprehensively. Specific study of procedures that obtained sufficient for various IoT was also investigated Requesting.

3.4.2 Privacy Efforts

Strong cryptographic steps have been used in previous studies, such as [56], to defend upon spiteful third multitudes, including to provide culpable IoT path. Nevertheless, as one of their tools, they didn't use either ML or BC. Kshetri et al. [7] demonstrated how compared to a conventional network for cloud-based services, BC techniques can provide better privacy-preserving solutions.

It also stressed BC's dominance in the management of identity and the establishment of admittance control. The research showed how using BC techniques, an invasion toward the IoT system could remain delimited. In this literature, though, a detailed privacy-preserving IoT fulmination pattern utilizing BC procedures was obtained needing. A short summary of IoT privacy concerns and problems, such as data sharing, was posed by Kumar et al. [54]. The work subsequently proposed BC-based explications over specific problems furthermore explored many sectors of application toward the implementation of BC. In contrast, the paper addressed BC's problems within every IoT utilization, which requires one detailed examination of IoT security and seclusion fulminations. These writers concerning [55] highlighted IoT solitude concerns furthermore presented their solutions based on BC. Attaining one "trio" regarding anonymity, unlinkability, moreover obstinacy was the prime purpose of privacy-preserving techniques. Based on conventional cryptographic techniques, the key security services, such as confidentiality, privacy and availability, have been discussed. The research harangued those impressions regarding IoT information distribution, information protection, moreover user behaviour and explored their solutions, such as data tagging, zero-knowledge evidence, pseudonyms, and the model of k-anonymity. In a conventional Identity Management (IdM) scheme, Zhu et al. highlighted privacy vulnerabilities, in particular because of their centralised architecture and reliability for so-called trusted third parties. Scarce seclusion interventions, before-mentioned being phishing also information leakage, can result in these vulnerabilities. The authors argued that due to certain fundamental IoT features such as scalability, versatility, and usability, standard IdM arrangements could no transpire explicitly emigrated until IoT ecosystems. The study further illustrated the privacy issues in conventional IdM systems and explored their BC-based solutions.

A comprehensive sketch regarding sequestration culmination in BC-based IoT policies was presented by Hassan et al. [57]. BC-based IoT network-related privacy attacks before-mentioned while Label reuse, Deanonymization, Charges by Sybil, Communications Spoofing, moreover Associating obtained highlighted. This trade further examined these implementations within BC-based implementations of the five diverse, widespread secrecy protection routines (Encryption, Smart Contract, Anonymization, Mixing, including Differential Privacy). The IoT privacy problems and their new BC-based solutions were analysed by Ali et al. [58]. Inside any centralised IoT paradigm before-mentioned records protection furthermore information confidentiality, they raised questions regarding privacy. Current centralised privacy solutions, such as the use of a privacy broker, the use of community signatures, the use of k-anonymity, and aliases, entirely rely profoundly covering third parties concerning their co-operations. The study provided a thorough analysis of the BC-based IoT privacy solutions to counter these problems.

3.5 Solutions to IoT Threats

Security experts have mitigated zero-day security, or privacy risks considering those commencements regarding one initial virus (Creeper) during 1970 before that Whatsapp scribbler proceeding 15 May 2019 and succeeding. Several solutions to mitigate protection and privacy problems have been suggested in this regard. However, within the aforementioned part, we concentrate upon particular latest paper recommending safe moreover privacy-preserving methods toward specific IoT specialties. We address significant explications given through primary utilizing ML algorithms essentially a guide, when over practicing BC methods, furthermore conclusively over merging both.

3.5.1 Existing Solutions Using Machine Learning (ML) Algorithms

ML implies we utilized in every application since each information processing pipeline. Notwithstanding instance, an ML prototype can dissect statistics traffic inserting a chain to kind an well-versed verdict. Figure 3.1 displays the key apparatuses of the ML hazard model for IoT. Additionally, for an attacker, the figure provides a survey concerning goal circumstances, before-mentioned since facts also output. Exploratory or poisoning attacks may occur on the information data of authorization upon IoT junctions and IoT junctions upon the ML design. Attacks of honesty and inversion are possible at performance [59]. Therefore, it must be protected as well as privacy-preserved for an entire system to be fully resistant to attacks.

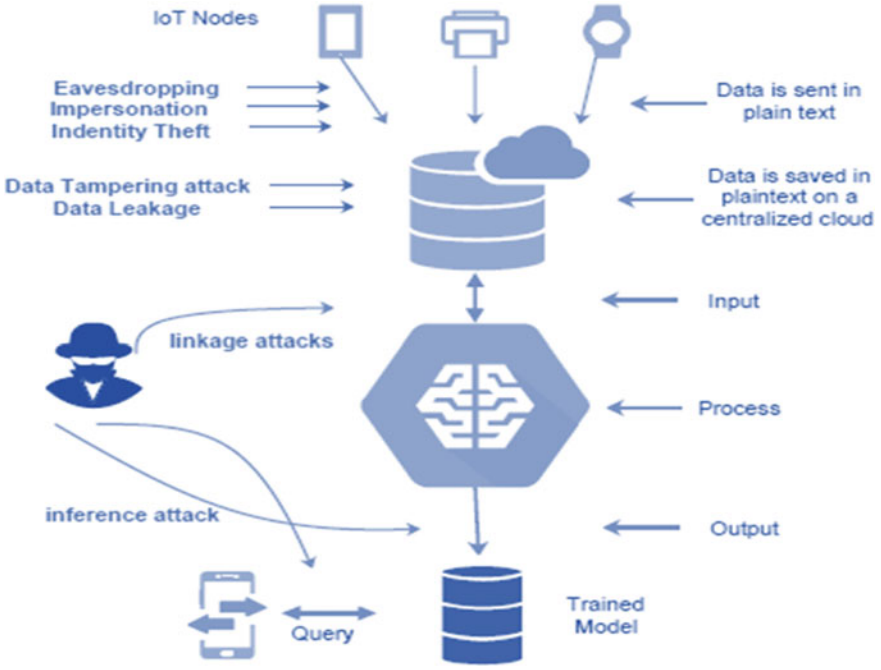


Fig. 3.1 An illustration of ML threat model for IoT

3.5.2 Existing Solutions Using Blockchain (BC) Technology

The BC network is protected, tolerant to errors, transparent, verifiable and auditable [60, 61]. Decentralized, P2P, open, trust-less, eternal, are the commonly used keywords to explain BC benefits. Such Features made a BC secure rather than a trusting fundamental client–server system. The smart convention is a BC programming protocol that ensures that a scheduled event is carried out [46]. The blockchain guarantees data integrity and authenticity, according to Restuccia et al. [42], making it an effective solution for defence against data tampering in IoT devices.

Several BC strategies for supply chain, identification, access and IoT management were suggested However, the current methods don't take into account time, and aren't applicable to resource-con IoT devices. And in comparison, other experiments examined time reaction of IoT devices, not just machado et al. [62] provided a three-layered architecture for Cyber-Physical Systems (CPS): an IoT (internal) architecture, a fog (external) design, and a cloud (external) design. First, IoT devices in the same network entity use the Proof-of-of-Trust (PoT) protocol (PoT). In IoT, Formal: Proof-of-of-Luck (PoL) was castoff to generate fault-tolerant cryptographic data, which provides an audit trail the first level's data was run via SHA-256 and temporarily stored. The consensus was achieved, and the data was saved at the third stage of the cloud which is a distributed ledger. Aside from data integrity, there were

also included the methods of key management and the node's position. The multi-lateration method was used to locate the node, and time synchronization was given by TSTP. It suggested the usage of various consents, like PoT and PoL, but ignored some privacy issues. Publication demonstrated a method of ensuring data privacy by utilizing public BC DroneChain introduced had four elements; the drones, the control system, the cloud, and the BC network. Drones were being operated by the controller, the data was processed and encrypted in the cloud using the decentralized BC. The resulting machine had accurate and up-to-date data with a fault-tolerant backend. The research however did not use Proof of Work (PoW), a real-time IoT application including drones notwithstanding. Additionally, the service did not have sidecoin data and encryption has not been seen to function. A DoS assault is one of the attacks that are widely used due to its simple implementation and the ever-increasing number of vulnerable computers. With the low cost of IoT technology, it is easy to get several machines under control to initiate an assault. The SDN is vulnerable to brute-force assaults. SDN is susceptible to attacks such as DoS/DDoS, because it is under the influence of machines. In a lightweight multi-standard IoT setting, earlier means of prevention may not be efficient. In addition to that, SDN is vulnerable to floods, saturation, MiTM assaults, and Man-in-the-the-middle.

attacks attributable to unauthenticated data in the unencrypted TCP channel Their formal argument has it that BC offers a stronger protection against the threats of network attacks and maintains confidence between multi-vendor devices; moreover, they asserted that BC is fault-tolerant and, tamper-proof. It is vulnerable to data tampering and flooding attacks because of these important attributes. However, all of the theories listed above were just theory; they've never been tried in practice. In a previous article, Sharma et al. enhanced protection in distributed SDN IoT proposed DistNet. This BC was used to ensure the current forwarding devices had the correct flow rule table checked, validated, and downloaded. DistNet's technologies were contrasted with those already in use, and the findings were higher in terms of real-time vulnerability monitoring and overhead. The researchers discovered a major protection loophole in the MiTM attack; a malicious attacker might alter user data that was transmitted across the internet with little difficulty. Furthermore, consumers were unable to scrutinize their expensive power bills since the grid was not equipped on early-with-early-warning functions. To prevent the above problems, this study suggested utilizing public and private keys and cryptographic data transfer on BC. The use of this methodology provided an eternal, stable, and transparent method. However, Proof of Work is not always cheap or resource-intensive.

It is claimed that the current logistics networks are neither simple nor dependable in [transparent and trustworthy]. Established networks were decentralized, leveraged several TTPs, and placed all their energy on a single point of energy transfer. Hasan et al. [57] introduced the BC distribution method. Nodes may be regarded as buyer, seller, courier services, as well as Smart Contract Verifier (SCAA). The contract was successfully put on Inter-Planetary File System (IPFS) and implemented after both the parties had come to an understanding. As per specifications of the object was moved between multiple transporters (maximum three times in this paper). When the object has been delivered and paid for, the customer releases the funds to the

vendor. If the deal is rejected, the arbitrator steps in, resolves the disagreement and redistributes the sum. The planned physical distribution method defends against Man-in-the-the-the-Middle and DOS threats. However, little regard has been given to manipulator ID administration or data privacy. In the paper by Gupta et al. [63], the writers appear to have dealt with phyical or programmatic Sybil attacks as well as the reiteration occurrences in an IoT network. The problem is not just because of the two additional layers in the current IoT design, but because they didn't have this latest one from the start. They clarified their algorithm, concept, and work in terms of transaction, block, and space use (Mmempool). IDS (now also known as Netflow) is one of the main ways to track unusual and malicious traffic patterns. The writers claimed in a report by Golomb et al. [64] that the new anomaly IDSs aren't effective because only innocuous traffic was used in the training process [64] Using this loophole, an adversary may introduce malicious data that is considered safe. Second, the qualified models could be lacking such event-driven IoT traffic, for example, including a fire alarm. Both of these questions is addressed using a CIoTA (Collaborative Internet of Things Anomaly) Detection approach, where all BC IoT devices of a since too many IoT devices were trained on their own traffic, there was a lower risk of an adversary assault. Any machine will form a locally trained model which would be collaboratively combined with other machines to form a globally trained model The CIo experiment proved to be an effective method for countering adversary assaults. However, the stand-alone model IoT node will, however, increase the volume of info. Complementing the study on widely studied risks such as Data privacy, as well as DoS mitm-based assaults, several remedies have been investigated. Sharma et al. introduced an inexpensive, always-on, and continuously-available methodology for cloud architecture. The introduction of SDN to the network along with BC was responsible for securing the fog nodes. To help maintain protection and also reduce end-to-to-end latency, the research study took the resource near to the IoT network. According to the developers, the model was flexible because of the observed risks and assaults, as well as streamlining the administrative procedures, it reduced their workload. The key goal of this paper was to create a BC-cloud architecture that was scalable, stable, and robust. It was measured in terms of production, reaction time, and false alarm. Nevertheless, there was no care given to either of data protection, user ID management, or key management was addressed. With regards to the unified infrastructure, Sharma et al. have maintained that the current Mobile Device Management (MDM) lacks robustness to security threats. They reported that their proposed system had increased latency, delay, and energy usage, while also keeping the original network architecture intact. Unfortunately, the thesis used Proof of Work (PoW) consensus, which is energy-hung and offers little consumer protection.

3.5.3 Existing Solutions Using Machine Learning (ML) and Blockchain (BC)

With the combination, Agrawal et al. reported to delete spoofing attacks ML algorithms and BC methods [65]. The user in a legitimate IoT-zone is constantly monitored by securing the user-device contact, and the BC is preserved in correspondence logs. Records are ongoing and repetitive events may be tracked. Current user authentication methods involve single-password (OTP) or safekeeping problems that are restricted to solo validation. Through using Distributed ledgers as that of the BC network, the researchers fixed the situation that use the IoT-zone recognition, IoT-token creation and the credential authentication. Nevertheless, the study found the Blockchain to be a communication core that reversed the notion of decentralization. No consumer or database protection was concerned and indeed the data collection for a Dnn models would be too small. Android's open nature raises new threats and attacks in terms of security. Gu et al. [66] illustrated that when examined overtime, the ransomware, Trojan horses, and extortion have targeted Android-based networks aggressively. Real programs, which may also be classified as non-linear analyses, get some drawbacks, including large computational time costs and styles of obfuscation of text, such as adjustable indoctrination and encrypting [67]. Gu et al. implemented a novel Multi Feature Based Paradigm (MFM), in which a malicious code index will be used by the BC Conglomerate for Malware Detection and Evidence Retrieval, on android platforms (CB-MDEE). In relation to past simulations, CD-MDEE obtained greater accuracy with decreased working time. The proposed architecture uses the Exonum BC platform and DNN ML algorithms to exploit BC's information sending and selling assets as and when needed to have management and future control of their health data [68]. The storage breach would not lead to data leakage, since the encrypted data in the store. In order to guarantee the acceptance and authenticity of the user records, the system utilizes hash features and public signature.

To maximise their target audience, many businesses rely on large datasets. However these information covers confidential private details, including political opinions that could be influenced and their profits raised by interested persons. Therefore, to protect and, if possible, protect the confidentiality of these customers, reimbursing them used for their donations is important. Moreover, a lot of evidence could be beneficial for design and technology in some dimensions, however the information can indeed be distributed with private entities. Moreover, this very same information collected can be modified and questions regarding their credibility can be raised. The above model has been improved by many reports. The proposal is [69, 70]. Mendis et al. [15] proposed that completely independent individual contributors cooperate de-centrally without interfering with their latter improved overall production efficiency and functionality [16]. In every case, over than 94% of the CNN sample size was compared with domain adaptation for the CNN model. The peer-to-peer transactions were conducted through smart contracts incentivizing the machine contributors. That being said, in their analysis [16], encoding time was increased by 100%. Furthermore, the construction was centered on the cryptocurrency BC having

a teaching effectiveness wedge time which might not be practicable, for examples for video transmission in a legitimate IoT program.

DeepChain proposed a value-driven, BC-based reward system for solving security problems. For the model training process, DeepChain guarantees data protection and auditability. Confidentiality is used for the Threshold Paillier algorithm, which gives a homomorphic additive property. Therefore more parties engaged in joint training, the greater the precision of training was shown by DeepChain, utilizing CNN protocols and MNIST datasets.

ML classification methods requires datasets in order to train. Because of multiple concerns surrounding confidentiality, including data theft, data confidentiality and custody, these databases are extracted from separate individuals, who usually do not want their communication to occur. Users are not sure of why and how their information will be used. In order to secure these confidentiality matters, Shen et al. [37] planned merging machine learning into cryptocurrency. A privacy-conserving SVM constructed classification had been cast-off to prepare the authenticated information obtained from Remote devices, although the BC system provided shared data between multiple service providers.

3.6 Deep Learning Approaches-Based IoT Data Privacy and Security

Throughout this section, detection equipment based on deep learning strategies are clarified. As seen in Fig. 3.2 There are ten supervised neural approaches used for detecting intrusion from information technology, namely (1) DNN; (2) FFDNN; (3) RNN; (4) CNN; (5) RBM; (6) DBN; (7) DA (Fig. 3.2);

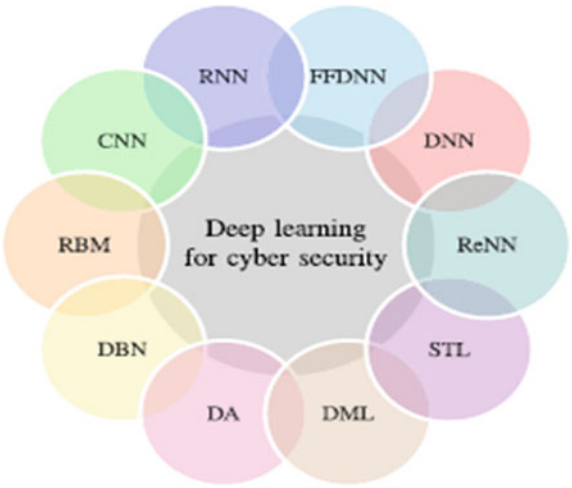


Fig. 3.2 Deep learning techniques used for intrusion detection in computer defense. FFDNN: Deep neuronal network feed forward; CNN: Convolutionary nerve-network; DNN: deep neural network; RNN: Recurrent neural network; DBN: Deep conviction network; STL: Self-tapping; ReNN: Neural network replicator. DBN: deep neural network

3.6.1 Deep Neural Network

Tang et al. [10] suggested a network monitoring approach that uses a deep learning approach for a software-defined framework. In the SDN controller which can monitor all openflux transitions the proposed Method framework is introduced. The study used the NSL-KDD 2-class (i.e. regular and phenomenon class) dataset, which involved of four classes, including four groups. (1) Attacking DoS, (2) attacking R2L, (3) attacking U2R, and (4) attacking sample. Exploratory findings found that the 0.001-learning threshold is more effective than others because of the receiver's largest operational curve (AUC). Potluri et al. [71] used this deep neural technique as a complex classifier for the management of enormous grid statistics. They just cast-off the NSL-KDD statistical model, which contains 39 detection techniques clustered in four inflammatory factors. Their analysis reveals that 2 classes had a good detection accuracy (i.e. normal and attack). Kang et al. [48] recommended an intrusion recognition process for vehicular networks founded on DNN. The scenario attack was carried out on malicious data packets which are inserted into the network bus of the in-vehicle controller region. To differentiate shipments into two categories (i.e., a regular packet in addition an outbreak packet), the proposed sys-temp inputs the function vector to the input nodes. Outputs are computed (e.g., ReLU) based on the activation function. Then, with these outputs, the next hidden layers are connected. The proposed system reaches a detection ratio of 99% if the untruthful optimistic fault is fewer than 1–2%. Zhou et al. [72] recommended an intrusion finding process founded on the DNN to help identify cyber-outbreaks. Specifically, three stages are used by the system, namely (1) DAQ, (2) data pre-processing, besides (3) deep classification of the neural network. For SVM model with a learning rate of 0.01, training epochs 10 and input elements 86, the stratagem accomplishes an accuracy of 0.963. The findings show this technique to marginally outperform the three methods to machine learning: (1) linear regression (LR), (2) random forest (RF), besides (3) k-nearest neighbourhood (KNN). Feng et al. [26] explains a plug-and-play framework using a network packet tool and mitigation paradigm that is used to track access denial (DoS) and ad hoc network incidents. The model suggested uses two types of in-depth processing, namely fully convolutional neural (CNN) as well as good memory for XSS and SQL challenges (LSTM). A deep neural network is used for the developed framework to detect DoS tacks. The survey was using the KDD CUP 99 database, which is split by 30% in evaluation and 70% in preparation. In comparison, the study reported an efficiency of 0.57 and 0.78% for the identification of XSS attacks by deep neural netting and convolutionary neural network.

A clear example of profound adversarial learning and predictive learning methods to detect net-work intrusions is the research by Zhang et al. [25]. By using data augmentation and advanced classification techniques, the analysis will classify a number of network intrusions. There are two elements used in the proposed method, the differential amplifier and the operator, in particular. The neural network is used as a predictor to reject enhanced infiltration information since actual illustrations while the compressor is used to produce expanded intrusion data. Kim et al. [73] worked

on data set from KDD in 1999 to run a deep neural network with ever-changing networks. In the suggested intrusion prevention scheme, design variables are used: four hidden layers and one hundred hidden units. ReLU is used as the initialization function as well as the simulated annealing mechanism for deep neural network testing. The classification results approximately 99% precision. Zhang et al. [46] have introduced a two-stage exploitation deletion method, known as CAN IDS, for detecting autonomous driving malicious attacks. In the first stage, a robust rule-based method is used, while for anomaly detection, the second stage uses deep learning net-work. Three datasets, including the Honda agreement, the Asian brand and the US brand car, are used in the assessment of results. Training database provides only regular traffic from all three sets, while testing set contain normal traffic and malicious activity, including falling strikes, direct attacks, zero-identification attacks, vulnerability scanning and spoof attacks.

3.6.2 Feedforward Deep Neural Network

For intrusion detection by Kasongo et al. [34], Feed forward deep neural network (FFDNN) was used. To create optimal subsets of features with minimal redundancy for wireless networks, Using FFDNN for a function selection technique dependent on target. The main training dataset was divided into 2 major sets i.e. data set for preparation and data set for evaluation) by the proposed intrusion detection system. Then a two-way process of normalisation and a process of feature transformation are involved. Finally, the pro-posed method utilises the FFDNN for model curriculum and research. The database NSL-KDD was castoff in addition the KDDTrain + and KD-DTest + were chosen. The estimation of results indicates that 99.69% including its proposed system with an operating rate of 0.05 and 30 neurons blowout over three hidden layers is correct.

3.6.3 Recurrent Neural Network

Kim et al.'s framework uses the KDD Cup database for the 1999 execution of a long, selective memory framework for a recurring neural remote monitoring model [74]. The effects were used as a feature vectors by the output vector (41 functions) (4 attacks and 1 non-attack). We also used step-by-step extent 100, load extent 50 also epoch 500. The intrusion optimal location is stated to be 98.8% across total attack occurrences. Loukas et al. [75] pro-posed a cyber-physical intrusion detection device to detect cyber attacks against vehicles. The method uses both the recurrent architecture of the NN and the DMP, highly efficient than conventional machine learning methods for high precision (e.g., k-means clustering and SVM). The computer is assessed against such a vehicle model using different categories of injection controls:

guidance attack, access denial intervention and perhaps a Network adapter vulnerability attack. Taylor et al. [1] suggested an anomaly detector to detect car algorithms rely on a recurrent neural network architecture. As a RNN, LSTM is used, which would be training to anticipate and its failures are used for detecting abnormalities new frame relay values. In an IDS method for supervised classification learning, Yin et al. [76] attempted to incorporate recurrent neural networking. The study used three performance metrics for the NSL-KDD dataset, this requires specificity, high false rates, and real positive rates. The consequence of outlier detection with a back propagation of = 0.1 and hidden neurons of = 80 is indicated as higher precision. The article also highlights the benefits of a repeating neural network for infiltration de-section schemes. Tang et al. [19] have suggested the use of a probabilistic neural unit, recurring mathematical computation for endpoint protection in software-defined networking. The paper reveals an 89% identification rate exploitation a minimal quantity of functions. The NSL-KDD dataset is being cast-off in network quality with four measurement parameters, i.e. recovery, F-Mail, precision and accuracy. Jiang et al. [20] has developed a cross intrusion detection method utilizing re-current neural networks for long-term memory. The NSL- KDD dataset is being cast-off for evaluating the effectiveness of the new outbreak recognition classification. The reliability of the reminiscence recall recurring neural networks is calculated at a speed of 99.23%, with a number of iterations of 9.86% and a precision of 98.94%.

3.6.4 Convolution Neural Network

Basumallik et al. [49] used convolutionary neural networks for packet-data anomaly detection in the state estimator based on phasor measurement units. To derive case fingerprints (features) from calculating units of phasor, they use a convolutionary neural network based data philtre. The IEEE-30 bus and IEEE-118 bus structures are being cast-off by means of phasor extent device buses. The analysis indicates a likelihood of 0.5 with a completely connected layer of 512 neurons and a precision of 98.67%. The authors say that, The neuronal philter is superior in its recital concluded all additional machine learning methods, namely RNN, LSTM, SVM, bagged then enhanced. The design constructed by Fu et al. [77] practices a convolutive neural network to monitor the inherent outlines of cheating events, in fact for the detection of credit card fraud. Zhang et al. [69] has used B2C banking institutions online transaction information for education and analysis, using the convolutionary network of neurons. One month's data was split into training sets and test sets. A 91% accuracy rate and a 94% recall rate are indicated in the report. These findings, relative to the work proposed by Fu et al. [77], are increased by 26% and 2% respectively. Nasr et al. [13] provided an invasion exposure classification, called DeepCorr, Centered on a convolutionary computer program to learn the role of differentiation. DeepCorr focuses mainly on two turnout layers and network layer of a fully linked neural network. Experimentation found that the unsurpassed recital is with a 0.0 0 01 learning rate, and with a false positives of 10–3, the DeepCorr reaches a true

positive rate similar to 0.8. Zhang et al. [78] introduced the model of a 2 layers neural network detection algorithm in which the primary layer is an improved neural network convolutionary LetNet-5 feature. Zhang et al. The upper method enables a long-term memory.

3.6.5 Restricted Boltzmann Machine

For intrusion detection, the constrained Boltzmann mechanism was castoff by Fiore et al. Towards syndicate the communicative ability of generative models with good classification, they use a discriminative restricted Boltzmann machine [79]. With a set of 41 traits and 97,278 examples, the KDD Cup 1999 dataset was used. Salama et al. [80] combine the Boltzmann restricted machine and the intrusion detection sup-port vector machine. The NSL-KDD dataset containing a total of 22 types of training attacks was used through an supplementary 17 kinds cutting-edge the difficult package. The training notes that a developed proportion of sorting is seen in this combination than by using the help vector machine. Alrawashdeh and Purdy [24] used the deep belief network of the restricted Boltzmann machine and hand-me-down the KDD 1999 information set comprising 494,022 training archives in addition 311,028 research records. C++ and Mi-crosoft Visual Studio 2013 are used to implement the detection algorithm. The research shows that 92% of attacks were categorised by the restricted Boltzmann machine. The paper combined the findings with Salama et al. [48work,]'s which shows both greater precision and speed of detection. Aldwairi et al. proposed a simulated study of Boltzmann limited hacker remote monitoring machines [81]. The analysis in specific demonstrates the efficiency of Boltzman restricted machines to discern among NetFlow traffic normal and anomalous. The research suggested was extended to the ISCX [82] database which had the maximum precision of 78.7 $\pm$ 1.9% so when study rates were set at 0.004. In comparison, the highest accuracy rates at the 0.004 learning scale are high, 74.9 ño 4.6% and 82.4 $\pm$ 1.8%. Gao and others are inclined and extended in the field of intrusion identification to the inclusion of multilayer unregulated training programs [83].The research is conducted using a limited Boltzmann machine with two levels of profound neural networking: (1) instruction of the Boltzmann machine on a small n-layer basis, and (2) fine tuning the whole Boltzmann machine parameter. The study reveals that the quality of the fully connected web on KDD CUP 1999 is greater than the quality of a vector supporting computer and a genetic algorithms built on the limited Boltzmann method. Alom et al. [64] identified an intrusion detection device that uses a stack-restricted Boltzmann computer. The main purpose of this strategy is to identify events that are Abnormal or malignant. The paper includes the NSL-KDD repository and is divided into five forms of attacks. The results reveal that the suggested solution achieves approximately 97.5% experiment precision at only 40% of the evidence used in testing. Yang et al. [84] therefore New approach suggested using the vector help machine, called SVM-RBM, based on restricted

Boltzmann machines, to provide enhanced traffic detection. For training functionality, the restricted Boltzmann computer is used. The authors continued to adjust the number of units in the hidden layers during the process of feature extraction. Then once the good features were obtained, the authors suggested that the trained prototype of a support vector process that uses the gradient downward algorithm with the trainable parameters. The SVM-RBMS algorithm suggested shows that perhaps the maximum precision approaches 80%.

3.6.6 Deep Belief Network

Thamilarasu et al. [40] used the deep-seated conviction framework for vulnerability scanning. They choose a deep belief network to develop a feed-forward-profile computer program for the IoT devices. The developers specifically introduced a binary interentropy prediction error in command to keep the overall cost of the IDS model to a minimum. The Keras archive, the Cooja Network Emulator and Texas Instruments CC2650 Sor markings are also used for process improvement. The Keras library is being castoff for the development of a procedural deep learning model. The theoretical prototypical was verified for 5 assaults (1) sinkhole, (2) wormhole, (3) blackhole assaults, (4) opportunistic service attack, and (5) DDoS attacks. The findings demonstration a 96% sophisticated meticulousness and a 98.7% reminiscence proportion for sleuthing DDoS outbreaks. Zhao et al. [85] in some other study, a based Protocols method utilizing the deep belief network and the cognitive deterministic network. The study contrasts the 10% learning database with the 10% reference data collection remote management model with the KDD CUP 1999 dataset. The findings show that it is stronger than three versions, namely (1) classical probability—based neural network, (2) the key component study of a generic probabilistic neural network, and (3) the non-optimized deep-faith network of the algorithm. Zhang et al. [63] analyzes are a prime example of how to incorporate enhanced genetic algorithms with a strong network of beliefs to predict computer security infringements. The study uses many restricted machines from Boltzmann which mainly lead to unsuited data learning. The profound beliefs framework is split into two phases in the performance evaluation: (1) each Boltzmann restricted computer is trained independently and (2) the whole last layer of that same deep beliefs network is formed as a network of neural proliferation. The NSL KDD database performance measurement suggests a detection rate of 99%.

3.6.7 Deep Auto-Encoder

The deep self-encoder has been cast-off by Shone et al. to identify interference in cyber protection [86]. In contrast with deep belief networks, to facilitate improved

classification performance, they are using an auto encoder with—anti different classifiers. The research uses five metrics per format datasets of the KDD Cup'99 and NSL-KDD, including precision, accuracy, false warning, F-score and recall. The test results for KDD Cup'99 suggest that an average of 97.85% of the developed framework can be higher than the work in [24]. In addition, the findings of the NSL-KDD data set assessment indicate that the counter model has reached a cumulative precision rate of 85%, an increase of 5% on the deep-beliew training algorithm. The two-phase deeper learning model has been used by Khan et al. [53] to propose a method of Intrusion Detection (TSDL). The TSDL framework contains a softmax auto module stacked with three primary layers (1), (2) the input layer, and (3) the output layer. A feed-forward neural network analogous to an inter sensor is employed by these three layers. Two public datasets, like KDD99 and UNSW-NB15, are being used in the analysis. High recognition rates, up to 99.996%, are reached by the KDD99 data set performance. Furthermore, up to 89.134% of the results on the UNSW-NB15 dataset reach high recognition rates. The use of auto-encoder techniques is proposed by Papamartzivanos et al. [67] Develop a detection system for peer and automatic violation assault. The proposed framework is explicitly based on four stages, including (1) tracking, (2) observing, (3) preparation, (4) exercise, and (5) information. The surveillance method decides any modification activity requiring an improvement to a sensor network. In order to convert raw traffic to real networks, the review program utilizes network auditing instruments (such as Argus and CICFlowMeter).

3.6.8 Deep Migration Learning

For cyber security intrusion detection, Li et al. are used for profound mobility learning [87]. The analysis explicitly integrates the deep learning model with the method of intrusion detection. Profound migration can be learned as per this article, four categories are divided, including the technical variable migration process, the simulation sample methodology, and the corresponding information migration methodology. The study utilises collection of KDD CUP 99 with 10% of the training examples as investigational information. Mostly throughout test, the study chooses the pooled haphazardly 10.0 0 0 data sets as classification model and the sampled 10.0 0 knowledge sets as the prototype test sets. The results show a 91.05% average precision and a untruthful positive rate of 0.56%.

3.6.9 Self-taught Learning

Javed et al. is using personality learning in order to detect information security attack. The suggested approach uses classification phases for the supervised learning except the overview of learning attributes and the obtained representation [88]. For validation

of findings the study uses the NSL-KDD dataset. The pro-position scheme contains three different forms of classification: (1) 2-class (i.e. ordinary and abnormal), (2) five-class (i.e. regular and four separate attack groups), and (3) 23-class (i.e. standard and 22 diverse outbreaks). The study used tenfold inter on formation data to determine the self-classification learning's consistency for those three modes of learning.

3.6.9.1 Replicator Neural Network

Cordero et al. [89] was using the cognitive replicator models to detect interference in cybersecurity. To locate anomalies, the analysis uses the dropout method. The extraction of entropy is composed of three steps. The aggregation of packets is the first level. The process consists of splitting the fluxes into service times. The final move is to collect those flows' fascinating features. The database is used to introduce inserting engineered attacks (e.g. SYN DDoS) into the information source for performance evaluation. The original data has been used.

3.7 Discussion of Taxonomy of Machine Learning Algorithms

Determining the role that each data set of data set serves in expanding an algorithm. You would still want to search for relevant or weird points of data to build up an algorithm features, as well as investigate value categories or hypotheses.

An unstructured dataset is typically best interpreted using clustering algorithms, which will aid in identification of form. Because K-means is the most commonly used and deals with a large volumes of data with a wide variety of data forms, it is able to provide significant performance when dealing with large volumes of data. Many [26] References (K and F together) have established a way to use the K-means algorithm for smart city and smart home data management (both long term and day-to-day data collection). Web databases, including the CitizensWire and The paraphrase: Oracle has also works for cluster database-scanning citizen web sources, which groups data found unlabeled these two databases by employing an Oracle-specific index, [5].

Using two techniques, odd and clever data points and anomaly-detection algorithms, it is possible to locate irregularities and strange facts in intelligent data of particular importance, these are one-instance and multilabel support vector machine learning (SVM) and spectral principal component analysis (PCA) techniques, which can both identify irregularities and poor or noisy data with excellent accuracy. Refs. [40, 85] used a single-class SVM to detect human behavior was considered to be effective in this task.

Two well accepted algorithms to make good predictions on and sequence data classified by the linear regression and the machine learning techniques were used. Data is usually consists of enormous quantities that need to be processed and trained

at a high speed to perform accurately. By example, in [83, 80] a simple regression algorithm was used for real-time prediction. An alternative that has proven useful for other rapid categorization and trend detection methods is the classification and regression tree, which has also been used to address problems with citizen behaviors.

To guess at the purposes, neural networks are an effective in helping to determine how various functions will be, they are well-suited learning models. Another reason for multi-class neural networks to have a good alternative is that it would take time to learn well and gather information to be of great accuracy. A good examples of FFNN use in use cases such as reducing potential energy demand include forecasting the data that will be produced and at future dates and how that data will be superseded, in each individual instances [use, as in which we see future redundancy in each specific instance is present on the list of items being removed] Another classification method, which is capable of managing enormous volumes of data and correctly classifying each of its categories, is the SVM Because of the capability of SVM to manage a large data sets and diverse kinds of features, it is widely used in various kinds of machine learning applications. Also, for example, the SVM was used to identify the results.

PCA and CA (both by the way of using a PC with an additional component and adding components to improve functionality) are two methods for enhancing the overall data features. Moreover, CCA is able to demonstrate a connection between two different types of data. Anomalies in a non-expanded PCA and CCA and non-PCA systems are often discovered using PCA and CCA techniques. For Reference [66], the PCA and CCA algorithms were applied to public areas and social venues to identify, capture, and record noteworthy data was developed.

The algorithm must be applied and designed correctly such that it arrives at a proper conclusion.

3.8 Research Challenges

3.8.1 Challenge to Machine Learning Algorithms in IoT

After practicing on several datasets, they may reasonably expected to the required performance, ML algorithms are used for analysis. For example, these models can be used in the navigation of a machine or language comprehension either that does not and could be used for individual know-how. To analyse threats against several cybersecurity domains, ML algorithms have also been used very efficiently. Although in many areas, they still have drawbacks on the Iot system: ML techniques rely well:

- **Scalability and Complexity**: In recent research some ML algorithms minimized cyber assaults successfully. That being said, Ai systems are not an optimal alternative for IoT implementations due to various their shortcomings. Diro et al. demanded that scalability, feature extraction, and accuracy of the traditional ML algorithms were restricted [34]. Whereas Moustafa et al. [31] argued that many

problems could not be solved by ML algorithms, Emotional and practical in a resource-restricted complex Distributed device. Another work of Abeshu et al. [27] shows that conventional ML algorithms are less efficient in addition less precise in a large distributed ledger including certain IoT. Various studies recently learned, after contrasting contemporary ML algorithms and DL methodologies, that most Modulus of elasticity use pretraining for dimensionality reduction. DL not just to avoided the problem, but also decreased the dimensionality of the function [54, 88, 90] by reducing repetition.

- **Latency**: Some authors, such as Xiao et al., have suggested using ensemble ML algorithms as a solution to the above problems. The aggregate theoretical framework superior than each Neural network independently, but computation was expensive. Most studies have pointed out as an alternative to classical ML, that DL is a better IoT choice.
- **Vulnerability**: Securing oneself from any security or privacy attacks is one of the main ML/DL strategies problems for IoT. Adversarial attacks may degrade system performance against machine learning models, as such attacks significantly decrease the accuracy of output [91]. The strength of the intrusion determines the amount of data given to the opponent of the method [71], which is very difficult to counter.

3.8.2 Challenges to Blockchain in IoT

- **Latency and speed**: While BC engineering was launched a era ago, its actual reimbursements have only been understood freshly. Numerous previous findings attempt to implement BC have included transportation, nutrition, electricity cities, VANET, 5G, wellbeing and operating expenditure in several applications. However, the current solutions do not meet latency concerns with BC and are not applicable to commodity IoT devices [19, 62]. PoW is the most common BC assumption, as seen in Table 10. PoW is sluggish and needs substantial resources (limited to 7 cycles per second, compared to the national average of 2000 network visa data per second).
- **Computation, processing, and data storage**: The maintenance of a BC across a vast network of peers [72] involves a substantial cost of computation, power, and memory. The size of the bitcoin ledger exceeded 196 GB in May 2018, according to Song et al. For an IoT device, these boundaries recommend underprivileged scaling in addition contract rapidity. Whilst it was an option to uploading the computing activities to a remote computer—cloud or quasi server—fog, there are still latencies throughout the network.
- **Compatibility and standardisation**: One of the BC challenges, like any emerging technology, is its standardisation, for which legislation needs to be renewed [90]. It would have been naive to expect that we all will see a degree of protection and privacy which will remove the chance of security breaches on IoT devices in the immediate future. Nevertheless a "reasonable" protection and privacy standards

can be ensured by a protocol specification. There are a range of essential protection and privacy features in every IoT system.

- **Vulnerability**: A decentralized framework is only as reliable as the platform's entry point even though the BC is non-repudiable, trustless, decentralised, and tamperproof. Anyone can access and view the content of data in a public BC-based scheme. While one of the solutions to the above problem is the private blockchain, other concerns are raised, such as trustworthy third parties, centralized management and user access regulation. In general, IoT solutions allowed to blockchain have to comply with either the security requirements like that of the data that I have to store for safe and confidential transmission; (ii) secure transmission of data; (iii) stable and responsible exchange of data; (iv) protection of identity and non-reputed properties; (iii) sharing of personal information; and Increasing the sharing of IoT solutions.

3.8.3 Challenges to Machine Learning (ML) and Blockchain (BC) in IoT

It is our view that a single device or tool, including such BC or ML, is not enough to provide maximum security and privacy for the IoT networks. The merger of BC and ML thus takes a long time for the scientific community to investigate the stability and anonymity of IoT.

Subsequent challenges:

- **Storage**: ML algorithms perform better with larger datasets, as discussed in Sect. 3.4 [27, 28]. That being said, the rise in BC's data will hinder its performance [70]. A simple research concern is the selection of a combination that will be suitable for IoT systems.
- **Latency challenges**: An IoT network can generate a significant amount of information depending on the scenario, more preparation and computation time is needed, which could theoretically boost the overall efficiency of typical Different classifiers (i.e. latency) [19, 62].
- **Scalability**: ML as well as BC have computation complexity both with respect to production and connectivity costs. Multiple ML algorithms place higher computing costs and connectivity costs as traffic increases, which is unavoidable for many of these IoT networks. Also, the BC is poorly managed with growing numbers of users and networking knots [76]. An Ethereum BC executes an increase of 11 transactions a second in standard IoT implementations, with bitcoin transactions taking place per second [62].
- **Selection of right algorithm**: The selection of correct algorithm is not limited to dozens, but a number of publicly accessible options are. There are basic rules that apply to all algorithm design projects: Algorithms should be used in all kinds of design scenarios, although there are exceptions to which one will be more appropriate. Expensively incorrect algorithm selection will result in useless

results or drag down the project over months of work, meaning that the efforts end result will be useless or will be delayed indefinitely.

- **The collection of data you are using for machine learning**: garbage in garbage out one must pay careful attention to the consistency, quantity, planning, and collection of the data used in machine learning projects to ensure their effectiveness. The data may be biased because of the following factors: The data must be carefully selected to prevent prejudice from influencing its results, and it is especially necessary to choose those who reflect all the events.
- **Data preparation**: The data has quality issues ranging from lost values to worthless values, which makes the results hard to trust and unreliable data is essential for data-normalization processes. Converting, truncation, refactoring, and cleaning of this data may be very time-consuming. Feature properties and feature requirements have to features should be studied and strategies including feature scaling has to be added to help avoid them dominating the blueprint.
- **Data Labelling**: are the ones used in supervised machine learning algorithms, which make the classification and recommendation processes both more straightforward and correct For a newly-implemented algorithm, unsupervised algorithm, this can be a very long and difficult operation, always involving many futile cycles of expanding and re-expanding. Only supervised machine learning algorithms need to be trained on labeled results. It's a job that requires plenty of effort, but outsourcing can't be trusted, so data marking must be done as part of the process. For example, health care services are a classic test of well-being because of the precariousness of their finances. Expanded vocabulary: In order for the predictive diagnosis to be effective, relevant medical evidence needs to be labelled. The marking relies on regular feedback from medical professionals and physicians but these people see the activity of labelling certain things like a trained doctors find it a waste of time.

In addition to these obstacles, there are plenty of others. Working with the developers, developing and maintaining product variants, creating and handling a separate copy of the results, and so on this is something that everybody employed on challenging projects knows about and understands: It's difficult to find good ML engineers, and if they constantly switching teams creates challenges for them, the job becomes overwhelming. It's an ongoing operation, and as time goes on. As time goes on, the system's specifications change, the algorithm should be given daily updates so it can have them as part of its environment.

Vulnerability: While ML and BC can significantly improve safety and confidentiality, there are also many challenges. On real time IoT platforms the difficulty of finding, working to prevent threats, namely malware and harmful programs, is growing. The ML training phase takes longer, and while malicious traffic can be detected, only a qualified model can do that [50]. Ledger will, but at the other hand, guarantee data non-repudiation and can understand their transformations. The dilemma, however, has been the compromised data before accessing the blockchain. Furthermore, the malfunction of sensing devices cannot be detected from the beginning before such a malfunction is established. The instrument [17] was tested. Besides

the aforementioned concerns, because the collected data are relevant to all stakeholders and is freely available, public BC is open to privacy infringement. One of the solutions to these challenges is the use of private BC, This will therefore restrict access to a considerable amount of information needed to successfully achieve ML [62].

3.9 Conclusion and Future Work

Throughout this segment, we discussed and categorized the latest risks to IoT as security and privacy. They briefly mentioned their consequences, type of actions, the interaction layer as well as the responses. We instead discussed and outlined the deficiencies in the new IoT regarding health and safety survey using both ML and BC architectures. This article provides the new IoT security and privacy strategies using Neural networks, BC methods and the implementation of both strategies. In order to better explain security and privacy issues in an IoT ML we have indeed attempted to present a regression analysis previous researcher. In conclusion, we have a range of study concerns on IoT Different classifiers, IoT BC approaches and IoT ML and BC mixture problems. The Digital gateway has essential for data collection, storage, study and correspondence. There is a performed a comprehensive, through initiatives such as adherence to best practises and continuous testing, where a vulnerability-free framework needs to be developed. As malicious activities are dynamic, the apparatus should be able to respond to the new hazard innovations (zero-day attacks). In this respect, in the study of traffic, ML/DL can be extremely helpful. At the same time, in an IoT environment, a log and correspondence directory will be maintained by the BC. As this information is unalterable, it can be used in the courts with trust as testimony. Majority of them should have concentrated on ensuring defense or anonymity in the fields of IoT defense and safety. We agree that both protection and privacy are equally necessary for a system to be secure. Moreover, the most important aspect is data protection, which can only be true when considered end-to-end. Present frameworks ignore the credibility of databases used only to create a network. These datasets can be tampered with by any opponent to achieve their desired performance. Currently, ML algorithms are being combined with BC techniques to achieve IoT protection and Privacy, which needs more exploration, is a relatively new field. Any concerns concerning analysis, however are: By mixing it, I could use BC with ML algorithms to eradicate DDoS attacks on an IoT network? (ii) Can the resource-constrained IoT system exploit the inherited encryption of BC for real-time performance? (iii) Can BC create trust in conventional IoT Intrusion Prevention Mechanisms based on collaborative ML? In addition, many organisations depend on the data generated by IoT devices, both public and private. Whether in motion or at rest, how can we trust the data? In a centralised IoT architecture based on the cloud, this question becomes more difficult to address. We significant data can be derived ML algorithms that secure privacy, while BC should maintain protection and trust. We plan to build

and create a privacy-preserving IoT platform in the future, which will provide data sharing and privacy-preserving data analysis to preserve privacy.

References

1. Taylor, A., Leblanc, S., Japkowicz, N.: Anomaly detection in automobile control network data with long short-term memory networks. In: 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA). IEEE; 2016. pp. 130–9
2. Cicds2017 Dataset. https://www.unb.ca/cic/datasets/ids-2017.html. Last Accessed 30 May 2019
3. Hidayet Aksu, A., Uluagac, S., Bentley, E.: Identification of wearable devices with bluetooth. IEEE Trans. Sustain. Comput. **2018**, 1–1 (2018)
4. Song, H., Fink, G.A., Jeschke, S.: Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications, pp. 1–472. Wiley
5. Goel, V., Perlroth, N.: Yahoo Says 1 Billion User Accounts Were Hacked. (2016). https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html
6. Peterson, A.: eBay asks 145 million users to change passwords after data breach (2014). https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/
7. Kshetri, N.: Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy **41**(10), 1027–1038 (2017). https://doi.org/10.1016/j.telpol.2017.09.003
8. Giles, M.: Five emerging cyber-threats to worry about in 2019. (2019). https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/
9. Milosevic, J., Malek, M. and Ferrante, A.: A friend or a foe? Detecting malware using memory and CPU features. In: Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016), vol. 4. pp. 73–84
10. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P.: Network intrusion detection for IoT security based on learning techniques. IEEE Commun. Surv. Tutor. **21**(3), 2671–2701 (2019)
11. Dartmann, G., Song, H., Schmeink, A.: Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things. Elsevier, pp. 1–360 (2019)
12. Aonzo, S., Merlo, A., Migliardi, M., Oneto, L., Palmieri, F.: Low-resource footprint, data-driven malware detection on android. IEEE Trans. Sustain. Comput. **3782**, c, 1–1 (2017). http://ieeexplore.ieee.org/document/8113505/
13. Nasr, M., Bahramali, A., Houmansadr, A.: Deepcorr: strong flow correlation attacks on TOR using deep learning. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018. pp. 1962–76
14. Ferdous, M.S., Chowdhury, M.J.M., Biswas, K., Chowdhury, N., Muthukkumarasamy, V.: Immutable autobiography of smart cars leveraging blockchain technology. Knowl. Eng. Rev. **22**, e3 (2020)
15. Song, J., Takakura, H., Okabe, Y.: Description of Kyoto University Benchmark Data; 2006. Available at link: http://www.takakura.com/Kyoto_data/ BenchmarkData-Description-v5.pdf. Accessed on 15 March 2016
16. Mawi Dataset. http://www.fukuda-lab.org/mawilab/data.html. Last Accessed 30 May 2019
17. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Fut. Gener. Comput. Syst. **88**, 173–190 (2018)
18. Price, W.N., Cohen, I.G.: Privacy in the age of medical big data. Nat. Med. **25**(1), 37–43 (2019). https://doi.org/10.1038/s41591-018-0272-7
19. Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R., Ghogho, M.: Deep recurrent neural network for intrusion detection in SDN-based networks. In: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018. pp. 202–6

20. Jiang, F., Fu, Y., Gupta, B.B., Lou, F., Rho, S., Meng, F., et al.: Deep learning based multichannel intelligent attack detection for data security. IEEE Trans. Sustain. Comput. (2018)
21. Hussain, F., Hassan, S.A., Hussain, R., Hossain, E.: Machine learning for resource management in cellular and IoT networks: potentials, current solutions, and open challenges. IEEE Commun. Surv. Tutor. C **2020**, 1–1 (2020)
22. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P., Ni, W.: Anatomy of threats to the Internet of Things. IEEE Commun. Surv. Tutor. **21** (2), 1636–1675 (2019)
23. Brass, I., Tanczer, L., Carr, M., Elsden, M., Blackstock, J.: Standardising a moving target: the development and evolution of IoT security standards. In: Living in the Internet of Things: Cybersecurity of the IoT, pp. 1–9
24. Alrawashdeh, K., Purdy, C.: Toward an online anomaly intrusion detection system based on deep learning. In: 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE; 2016. pp. 195–200
25. Zhang, H., Yu, X., Ren, P., Luo, C., Min, G.: Deep adversarial learning in intrusion detection: a data augmentation enhanced framework (2019). arXiv preprint, arXiv: 1901.07949
26. Feng, F., Liu, X., Yong, B., Zhou, R., Zhou, Q.: Anomaly detection in ad-hoc net- works based on deep learning model: a plug and play device. Ad Hoc Netw. **84**, 82–89 (2019)
27. Abeshu, A., Chilamkurti, N.: Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag 56(2):169–175 (2018)
28. Elejla, O.E., Belaton, B., Anbar, M., Alabsi, B., Al-Ani, A.K.: Comparison of classification algorithms on ICMPv6-based DDoS attacks detection. Lect. Notes Electr. Eng. **481**(2019), 347–357 (2019)
29. Otoum, S., Kantarci, B., Mouftah, H.: Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In: 2018 IEEE International Conference on Communications (ICC). IEEE; 2018, pp. 1–6
30. Rezazad, M., Brust, M.R., Akbari, M., Bouvry, P., Cheung, N.M.: Detecting target-area link-flooding DDoS attacks using traffic analysis and supervised learning. Adv. Inf. Commun. Netw. 180âĂŞ202 (2018). https://doi.org/10.1007/978-3-030-03405-4_12
31. Moustafa, N., Turnbull, B., Choo, K.K.R.: An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. IEEE IoT J. **6**(3), 4815–4830 (2019)
32. Diro, A., Chilamkurti, N.: Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Commun. Mag. **56**(9), 124–130 (2018)
33. Roy, D.G., Das, P., De, D., Buyya, R.: QoS-aware secure transaction framework for internet of things using blockchain mechanism. J. Netw. Comput. Appl. **15**(144), 59–78 (2019)
34. Kasongo, S.M., Sun, Y.: A deep learning method with filter based feature engineering for wireless intrusion detection system. IEEE Access **7**, 38597–38607 (2019)
35. Ahmad, U., Song, H., Bilal, A., Saleem, S., Ullah, A.: Securing insulin pump system using deep learning and gesture recognition. In: Proceedings—17th IEEE international conference on trust, security and privacy in computing and communications and 12th IEEE international conference on big data science and engineering, Trustcom/BigDataSE 2018:1716–1719 (2018)
36. D., Maity, S., Sen, S.: 2018. RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. In: Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018, c (2018), pp. 205–208
37. Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M.: Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet Things J. **2019**, 1–1 (2019)
38. Azmoodeh, A., Dehghantanha, A., Choo, K.K.R.: Robust malware detection for internet of (Battlefield) things devices using deep Eigen space learning. IEEE Trans. Sustain. Comput. **3782**, c, 1–1 (2018). http://ieeexplore.ieee.org/document/8302863/
39. Fu, K., Cheng, D., Tu, Y., Zhang, L.: Credit card fraud detection using convolutional neural networks. In: International Conference on Neural Information Processing, 2016. pp. 483–90. Springer

40. Thamilarasu, G., Chawla, S.: Towards deep-learning-driven intrusion detection for the internet of things. Sensors **19**(9), 1977 (2019)
41. Al-Rubaie, M., Chang, J.M.: Privacy preserving machine learning: threats and solutions. IEEE Security and Privacy Magazine (2018)
42. Restuccia, F., D'Oro, S., Melodia, T.: Securing the Internet of Things in the age of machine learning and software-defined networking. IEEE IoT J. **1**(1), 1–14 (2018)
43. Sharmeen, S., Huda, S., Abawajy, J.H., Ismail, W.N., Hassan, M.M.: Malware threats and detection for industrial mobile-IoT networks. IEEE Access **6**(2018), 15941–15957 (2018)
44. da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque, V.H.C.: Internet of Things: a survey on machine learning-based intrusion detection approaches. Comput. Netw. **151**, 147–157 (2019). https://doi.org/10.1016/j.comnet.2019.01.023
45. Ji, Z., Lipton, Z.C., Elkan, C.: Differential privacy and machine learning: a survey and review. CoRR abs/1412.7584 (2014). http://arxiv.org/abs/1412.7584
46. Zhang, L., Shi, L., Kaja, N., Ma, D.: A two-stage deep learning approach for can intrusion detection. In: Proceedings Ground Vehicle systems Engineering and Technology Symposium (GVSETS), pp. 1–11 (2018)
47. Fernández-Caramés, T.M., Fraga-Lamas, P.: A review on the use of blockchain for the Internet of Things. IEEE Access **6**(2018), 32979–33001 (2018)
48. Kang, M-J., Kang, J-W.: Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE, **11**(6), e0155781 (2016)
49. Ferrag, M.A., Maglaras, L.: Deepcoin: a novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Trans. Eng. Manage. (2019)
50. Center for Applied Internet Data Analysis. https://www.caida.org/data/overview/. Last Accessed 30 May 2019
51. Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for internet of things security: a position paper. Digit. Commun. Netw. 4(3):149–160 (2018). https://doi.org/10.1016/j.dcan.2017.10.00
52. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Fut. Gener. Comput. Syst. **82**, 395–411 (2018). https://doi.org/10.1016/j.future.2017.11.022
53. Khan, F.A., Gumaei, A., Derhab, A., Hussain, A.: Tsdl: a two stage deep learning model for efficient network intrusion detection. IEEE Access (2019)
54. Kumar, N.M., Mallick, P.K.: Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. **132**, 1815–1823 (2018). https://doi.org/10.1016/j.procs.2018.05.140
55. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: a top-down survey. Comput. Netw. **141**, 199–221 (2018). https://doi.org/10.1016/j.comnet.2018.03.012
56. Ferretti, L., Longo, F., Colajanni, M., Merlino, G., Tapas, N.: Authorization transparency for accountable access to IoT services. In: Proceedings—2019 IEEE International Congress on Internet of Things, ICIOT 2019—Part of the 2019 IEEE World Congress on Services (2019), pp. 91–99
57. Hassan, M.U., Rehmani, M.H., Chen, J.:. Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. Fut. Gener. Comput. Syst. **97**, 512–529 (2019). https://doi.org/10.1016/j.future.2019.02.060
58. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2):1676–1717 (2019)
59. Lbnl Dataset. https://powerdata.lbl.gov/download.html. Last Accessed 23 Juin 2019
60. Baxter, R., Hastings, N., Law, A., Glass, E.J.: Future Uses of Blockchain. vol. 39, pp. 561–563. https://www.thestreet.com/technology/cybersecurity/five-future-uses-for-blockchain-14589274
61. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016). http://ieeexplore.ieee.org/document/7467408/
62. Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: review and open research challenges. IEEE Access **7**, 10127–10149 (2019)

63. Zhang, Y., Li, P., Wang, X.: Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access **7**, 31711–31722 (2019)
64. Alom, M.Z., Bontupalli, V., Taha, T.M.: Intrusion detection using deep belief networks. In: 2015 National Aerospace and Electronics Conference (NAECON). IEEE, 2015. pp. 339–44
65. Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S.A., Shekhar, S.: Continuous security in Iot Using Blockchain 6423–6427 (2018)
66. Gu, J., Sun, B., Du, X., and Senior Member.: Consortium blockchain-based malware detection in mobile devices. IEEE Access **6** (2018)
67. Ikram, M., Beaume, P., Kâafar, M.A.: DaDiDroid: an obfuscation resilient tool for detecting android malware via weighted directed call graph modelling. In: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, Prague, Czech Republic, July 26–28, 2019. SciTePress, pp. 211–219. https://doi.org/10.5220/0007834602110219
68. Homoliak, I., Barabas, M., Chmelar, P., Drozd, M., Hanacek, P.: ASNM: advanced security network metrics for attack vector description. In: Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer âQ; 2013. p. 1
69. Feng, P., Ma, J., Sun, C., Xu, X., Ma, Y.: A novel dynamic android malware detection system with ensemble learning. IEEE Access **6**(2018), 30996–31011 (2018)
70. Song, J.C., Demir, M.A., Prevost, J.J., Rad, P.: Blockchain design for trusted decentralized IoT networks. In 2018 13th System of Systems Engineering Conference, SoSE 2018
71. Potluri, S., Diedrich, C.: Accelerated deep neural networks for enhanced intrusion detection system. In: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE; 2016. pp. 1–8
72. Zhou, L., Ouyang, X., Ying, H., Han, L., Cheng, Y., Zhang, T.: Cyber-attack classification in smart grid via deep neural network. In: Proceedings of the 2nd Inter- national Conference on Computer Science and Application Engineering. ACM; 2018. p. 90
73. Kim, J., Shin, N., Jo, S.Y., Kim, S.H.: Method of intrusion detection using deep neural network. In: 2017 IEEE International Conference on Big Data and Smart Computing (BigComp). IEEE, 2017. pp. 313–16
74. Roy, D.G., Das, M., De, D.: Cohort assembly: a load balancing grouping approach for traditional WiFi infrastructure using edge cloud. In: Methodologies and Application Issues of Contemporary Computing Framework 2018 (pp. 93–108). Springer, Singapore
75. Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D.: Cloud-based cy- berphysical intrusion detection for vehicles using deep learning. IEEE Access **6**, 3491–3508 (2017)
76. Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access **5**, 21954–21961 (2017)
77. Basumallik, S., Ma, R., Eftekharnejad, S.: Packet-data anomaly detection in PMU-based state estimator using convolutional neural network. Int. J. Electric. Power Energy Syst. **107**, 690–702 (2019)
78. Zhang, Y., Chen, X., Jin, L., Wang, X., Guo, D.: Network intrusion detection: based on deep hierarchical network and original flow data. IEEE Access **7**, 37004–37016 (2019)
79. Roy, D.G., Mahato, B., De, D., Buyya, R.: Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols. Futur. Gener. Comput. Syst. **1**(89), 300–316 (2018)
80. Salama, M.A., Eid, H.F., Ramadan, R.A., Darwish, A., Hassanien, A.E.: Hybrid intelligent intrusion detection scheme. In: Soft Computing in Industrial Applications, 2011. pp. 293–303, Springer
81. Aldwairi, T., Perera, D., Novotny, M.A.: An evaluation of the performance of restricted Boltzmann machines as a model for anomaly network intrusion detection. Comput. Netw. **144**, 111–119 (2018)
82. Jing, X., Yan, Z., Jiang, X., Pedrycz, W.: Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch. Inf. Fusion **51**, 100–113 (2019). https://doi.org/10.1016/j.inffus.2018.10.013

83. Gao, N., Gao, L., Gao, Q., Wang, H.: An intrusion detection model based on deep belief networks. In: 2014 Second International Conference on Advanced Cloud and Big Data. IEEE; 2014. pp. 247–52
84. Yang, J., Deng, J., Li, S., Hao, Y.: Improved traffic detection with support vector machine based on restricted Boltzmann machine. Soft Comput. **21**(11), 3101–3112 (2017)
85. Zhao, G., Zhang, C., Zheng, L.: Intrusion detection using deep belief network and probabilistic neural network. In: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), vol. 1. IEEE; 2017. pp. 639–642
86. Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q.: A deep learning approach to network intrusion detection. IEEE Trans. Emerg. Top. Comput. Intell. **2**(1), 41–50 (2018)
87. Javaid, A., Niyaz, Q., Sun, W., Alam, M.: A deep learning approach for network intrusion detection system. In: Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies; 2016, pp. 21–6
88. Roy, D.G., Mahato, B., De, D.: A competitive hedonic consumption estimation for IoT service distribution. In: 2019 URSI Asia-Pacific Radio Science Conference (AP-RASC) 2019 Mar 9, pp. 1–4. IEEE
89. Iscx Dataset. https://www.unb.ca/cic/datasets/ids.html. Last Accessed 23 Juin 2019
90. Niwa, H.: Why Blockchain is the future of IoT? (2007). https://www.networkworld.com/article/3200029/internet-of-things/why-blockchain-is-the-future-of-iot.html
91. Roy, D.G., Mahato, B., Ghosh, A., De, D.: Service aware resource management into cloudlets for data offloading towards IoT. Microsyst. Technol. **4**, 1–5 (2019)