This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3089681, IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Security Threats and Artificial Intelligence based Countermeasures for Internet of Things Networks: A Comprehensive Survey

SHAKILA ZAMAN[1], KHALED ALHAZMI[2], MOHAMMED ASEERI [3], MUHAMMAD RAISUDDIN AHMED [4], (Member, IEEE), RISALA TASIN KHAN[5], (Senior Member, IEEE), M. SHAMIM KAISER[5], (Senior Member, IEEE),MUFTI MAHMUD[6,7], (Senior Member, IEEE)

[1]Department of CSE, BRAC University, Dhaka, Bangladesh (e-mail: shakila.zaman@bracu.ac.bd)
[2]National Center for Robotics and Internet of Things Technology, Communication and Information Technology Research Institute, King Abdulaziz City for Science and Technology (KACST), Riyadh, Saudi Arabia (e-mail: khazmi@kacst.edu.sa)
[3]National Center for Robotics and Internet of Things Technology, Communication and Information Technology Research Institute, King Abdulaziz City for Science and Technology (KACST), Riyadh, Saudi Arabia (e-mail:masseri@kacst.edu.sa)
[4]Radio and Radar, Communication, Military Technological College, Muscat, Oman (e-mail: rais80@yahoo.com)
[5]Institute of Information Technology, Jahangirnagar University, Savar, Dhaka 1342, Bangladesh (e-mail: {risala,mskaiser}@juniv.edu)
[6]Department of Computer Science, Nottingham Trent University, NG11 8NS – Nottingham, UK
[7]Medical Technologies Innovation Facility, Nottingham Trent University, NG11 8NS – Nottingham, UK (e-mail: mufti.mahmud@ntu.ac.uk, muftimahmud@gmail.com)

Corresponding authors: Khaled Alhazmi (khazmi@kacst.edu.sa) and Mufti Mahmud (muftimahmud@gmail.com, mufti.mahmud@ntu.ac.uk)

ABSTRACT The Internet of Things (IoT) has emerged as a technology capable of connecting heterogeneous nodes/objects, such as people, devices, infrastructure, and makes our daily lives simpler, safer, and fruitful. Being part of a large network of heterogeneous devices, these nodes are typically resource-constrained and became the weakest link to the cyber attacker. Classical encryption techniques have been employed to ensure the data security of the IoT network. However, high-level encryption techniques can not be employed in IoT devices due to the limitation of resources. In addition, node security is still a challenge for network engineers. Thus, we need to explore a complete solution for IoT networks that can ensure nodes and data security. The rule-based approaches and shallow and deep machine learning algorithms– branches of Artificial Intelligence (AI)– can be employed as countermeasures along with the existing network security protocols. This paper presented a comprehensive layer-wise survey on IoT security threats, and the AI-based security models to impede security threats. Finally, open challenges and future research directions are addressed for the safeguard of the IoT network.

INDEX TERMS Fuzzy logic, Machine Leaning, Attack Vector, IoT Protocols, IoT Applications.

I. INTRODUCTION

WITH the rapid amelioration of the low-cost sensing devices and cloud/fog-based computing techniques, IoT–which interconnects smartest physical attributes and intelligent virtual interfaces—-has outrivaled the conventional sensing technique. IoT nodes can communicate with each other and react autonomously without human interaction [1]. Due to efficiency and autonomous characteristics, IoT applications have been increased in every aspect of life. Integration of heterogeneous nodes in IoT network has raised security concern.

IoT is adopted in a wide variety of applications including smart home [2], smart office [3], [4], automated industry [5], smart city [6] intelligent farming and agriculture [7], intelligent transportation systems [8], supply chain [9], smart healthcare [10], etc. In these applications, IoT nodes utilize various sensors to collect the data from the environment and send to the embedded devices. These nodes are constrained for computing capabilities and transfers data to fog and/or cloud node via wire/wireless network for generating insights. During the transmission, IoT devices and network topologies are vulnerable and susceptible to security attacks.

IoT uses multiplayer architecture such as sensing, access, processing, application layers. Each layer of IoT relies on individual security scheme and protection flaws, which are really challenging to address and provide an appropriate countermeasure [11].

Zhen Ling et al. [12] demonstrated a case study of the ineptitude of IoT devices in the mitigation of an attack by installing Edinax SP-2101W in an iPad and able to launch common attacks, such as device scanning attack, brute force attack, spoofing attack, and firmware attack. Authors also showed that IoT node resources were insufficient to incorporate complex encryption technologies. Therefore, security and privacy handling in IoT networks are one of the most significant challenges.

When an IoT system is compromised, attackers can not only access confidential data collected by IoT nodes, but can also interrupt the regular activity of the IoT network. This lack of confidentiality, integrity and data security in IoT will disrupt widespread adoption of this technology. Yang et al. [13] Tewari and Gupta [14], and Lin et al. [15] discussed some well-known IoT security threats such as spoofing, Man-in-the-Middle (MITM) attack, hardware threats, cloning the data access, eavesdropping, device tampering, signal jamming, Distributed Denial of Service (DDoS), back-off manipulation, granted time slots, malicious code injection, sybil attack, side-channel attack, reply attack, physical damage, tag cloning, information leak, etc.

The conventional symmetric and asymmetric security protocols developed by several researchers, such as Advanced Encryption Standard (AES) [16], Hash function [17], signature-based Intrusion detection [18], Elliptic Curve Cryptography (ECC) [19], Public Key Infrastructure (PKI) [20], Secure Shell Algorithm (SSH) [21], Rivest Shamir-Adleman (RSA) [22], Data Encryption Standard (DES) [23], Rivest Cipher (RC6) [24], and Triple DES (3DES) [25], are widely used for ensuring secure access to communication systems. These algorithms are robust, but require tremendous resources (memory and computing) and drain more power and may not be suitable for providing security in resource constrain IoT network. In the last decade, however, researchers have proposed a large number of lightweight primitives for resource-restricted IoT networks [26] such as lightweight version of Data Encryption Standard (DESL) [27], DESXL [28], Tiny Encryption Algorithm (TEA) [29], etc. The main issue of a lightweight encryption algorithm is poor performance accuracy in terms of dynamic security threats in a low resource setting.

On the other hand, AI and Machine Learning (ML) techniques are notable for their predictive abilities in a number of fields such as anomaly detection [30]–[33], biological data mining [34], [35], cyber security [36], disease detection [37]–[45], earthquake prediction [46], elderly care [47], [48], elderly fall detection [49]–[51], financial prediction [52], safeguarding workers in workplaces [53], text analytics [54], [55], and urban planning [56].

Thus, bio / brain-inspired and shallow / deep learning (DL) based models can also be used to to detect and predict attacks on IoT networks.

It is, therefore, remarkable that AI based countermeasure solutions are increasingly essential to improve security performance. In order to address this gap and mitigate the problem, this paper presents a comprehensive study of possible layer-wise security threats and identifies AI based security solutions.

In this study, we explored published articles related to security Threats and AI based countermeasures in well-known databases such as IEEE Xplore digital library, Science Direct, and Google Scholar. Out of the initially reported 751 journal and conference papers over the last decade, 525 articles were chosen for full-text review after removing duplicate entries and reviewing the abstract. After reading the full report, 475 papers were omitted from the study and only 150 articles were eventually chosen. Fig. 1 and fig. 2 shows the rest of the paper taxonomy and a word cloud where, most frequent words are counted in the area of IoT network security. The contribution of this work is listed below:

- The layer-by-layer IoT protocols and corresponding security threats has been discussed in this research.
- An extensive survey is presented on the use of rule-based methods (such as Fuzzy Logic (FL) and Neuro-Fuzzy System (NFS)); shallow ML algorithms (such as Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), Decision Tree (DT), Naive Bayes (NB), Q-Learning, Multilayer Perceptron (MLP)) and DL algorithms (such as Convolutional Neural Network (CNN), Deep Q Network (DQN), Deep Neural Network (DNN), Recurrent Neural Network (RNN), Long Short Term Memory (LSTM); Extreme Gradient Boosting (EGB)) for countermeasure of the layer wise threats.
- The performance of these AI based countermeasure algorithms has been listed.
- The researech limitation, open challenges, and future research directions are highlighted.

Other sections are arranged as– Section 2 discusses related IoT threats and countermeasure found in the existing review papers. Section 3 presents IoT architecture and also offers the features for every layer; Section 4 explains layer-wise security threats. AI/ML based counter measurements are identified in Section 5. Section 6 addresses the emerging open security problems and provides potential research guidelines for IoT networks.

II. RELATED REVIEW WORKS

In the last couple of years, many researchers have conducted reviews on existing IoT security countermeasures to provide a road-map for future work. Due to the heterogeneity of IoT networks, an intruder may create dynamic threats to take control of authorized communications or hardware devices. This section represents IoT security-related review papers.

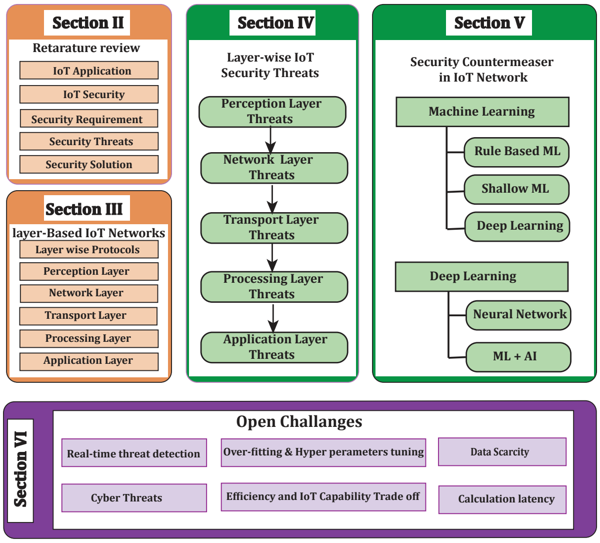

FIGURE 1. Taxonomy of this article. Section II and III represent mostly the related review works and IoT network characteristics. Security threats and AI-based countermeasures are discussed in section IV and V. Challenges of implementing AI in IoT security are listed in section VI.

FIGURE 2. Word Cloud identified keywords contained in article title discussed in the the literature survey and methodology section.

Ali et al. [57] reviewed layerwise security attacks and their level of impact on IoT network along with the traditional symmetric and asymmetric encryption algorithms for user authentication and access control. The work also addressed various challenges to conventional security solution. Andrea et al. [58] conducted a survey on IoT security goals and provided an unique classification of IoT attacks consisting physical Attacks, Network Attacks, Software Attacks and Encryption Attacks. Encryption-based security countermeasures are highlighted to direct the future work of security in heterogeneous IoT environment. For instance, cryptography hash is addressed for secure booting, device authentication, data integrity, routing security, and data security. Deep et al. [59] reviewed the layered context of IoT security along with the challenges and fundamental security requirements against various attacks like node capture, fake node, Mass node authentication, DDoS etc. The work also listed advantages and disadvantages of existing conventional security mechanisms in perception layer, network layer, middle layer and application layer. Kouicem et al. [60], and Granjal et al. [61] analyzed conventional encryption mechanisms to ensure the key security requirements like authentication, availability and confidentiality in case of various attacks such as malicious code injection, IP spoofing, DoS/DDoS etc. where Kouicem et al. [60] refereed for advanced emerging technologies like Software Define Network (SDN) and Blockchain for enhanced security mechanism. Loukil et al. [4] represented a systematic study of transmitted data life cycles and evaluate the existing preserving techniques (For example anonymization, cryptography, access control) according to ISO privacy protocols specifically for Europe and address the limitation of cryptography. Suo et al. [62] paid attention to IoT security by intensely analyzing the layer-based security features, requirements, and common cryptography mechanisms against of MITM attack, counterfeit attack, DDoS, external attacks etc. for communication security and sensor data security. Moreover, the paper addressed the limitations and challenges of implementing conventional encryption techniques for heterogeneous IoT environments. Thuat et al. [63] reviewed key-based bootstrapping distributed approaches for various attacks like denial of service, DoS, and replay attacks. In addition to that by analyzing the limitation of the existing symmetric mechanism, this work suggested more intelligent lightweight public key cryptography to secure IoT communication. Hameed and Alomary [64] presented an overview of several types of IoT attacks and discussed extensively about the countermeasures against side-channel, hardware/software attacks. Authors found that light weight encryption algorithms are not adequate to secure dynamic IoT networks and are recommended for further security solution.

Sfar et al. [65] emphasized data privacy based on lightweight primitive block cipher (such as HIGHT, PRESENT, KLEIN, LED, mCRYPTON etc.), hash function (such as SQUASH, Keccak, Photon, GLUON, etc.), anonymization, stream cipher (such as Trivium, A2U2, Grain, MICKEY, Espresso, etc.) and public-key cryptography (such as ECC, Hyper-ECC, NTRU, etc.) to provide a systematic road-map for security challenges in IoT networks.

Surendran et al. [66] compared novel lightweight encryption algorithms for Windows / embedded system (e.g., DESL, DESXL, Katan, Ktantan. HIGHT, HIGHT2, PES, RSA, extended TEA etc.). The authors found that the ciphers were better suited to windows than embedded systems. Because of the device's unique features, existing software-based security protocols were often cumbersome and provided a new loophole for security.

Xiao et al. [67] briefly studied ML-based protection approaches to defending data privacy from unauthorized access and control of malware by considering different models of attack such as DoS/DDoS, jamming, spoofing, MITM, soft-

TABLE 1. Discussed issues / contents and considered countermeasures of IoT systems in existing works.

References	Year	Discussed issues/ contents	Considered security algorithms	Challenges
Ali *et al.* [57]	2019	Layer-wise security attacks	Symmetric / Asymmetric encryption algorithms.	Yes
Andrea *et al.* [58]	2015	Security goals and classification of various attacks	Encryption-based countermeasures.	No
Deep *et al.* [59]	2020	Layer-wise security attacks	Encryption-based countermeasures.	Yes
Kouicem *et al.* [60]	2018	Analyzed various security requirements	Encryption algorithms, SDN, Blockchain based countermeasures.	Yes
Loukil *et al.* [4]	2017	Security properties and requirements	Evaluate various preserving techniques (e.g. anonymization, cryptography, access control).	Yes
Suo *et al.* [62]	2012	Layer-wise security features and requirements	Cryptography algorithms against of MITM / counterfeit / DDoS / external attacks.	Yes
Thuat *et al.* [63]	2015	Security requirements and protocols of IoT network	Key-based bootstrapping distributed approaches.	Yes
Hameed and Alomary [64]	2019	Various types of IoT attacks	Light-weight encryption algorithms against side-channel and hardware/software attacks.	No
Sfar *et al.* [65]	2018	Emphasized on data privacy on IoT network	Lightweight block cipher, hash function, anonymization, stream / public-key cryptography.	Yes
Surendran *et al.* [66]	2018	Properties of IoT devices on Windows / embedded systems	Lightweight encryption algorithms.	No
Xiao *et al.* [67]	2018	Addressed various attacks	ML-based countermeasures.	Yes
Tahsien *et al.* [68]	2020	Analyzed passive and active attacks	Discussed shallow ML approaches.	Yes
Zeadally and Tsikerdekis [69]	2020	IoT device's properties and frequent attacks	Host-based and network-based ML based algorithms.	Yes
Gupta *et al.* [70]	2020	Categorized IoT attacks based on goal, performer, and layered	ML-based solutions for DoS, MITM and selective forwarding attacks.	No
Hasan *et al.* [71]	2019	Analyzed frequent attacks	ML-based countermeasures.	No
Amiri-Zarandi *et al.* [72]	2020	Layer-wise data sources of IoT Network	ML techniques to maintain IoT network privacy.	Yes
Mamdouh *et al.* [73]	2018	Classification of IoT and WSN based frequent security attacks	Shallow ML based countermeasures.	No
Hussain *et al.* [74]	2019	Provide classification of various attacks	ML and DL based solutions to overcome challenges of traditional cryptography.	Yes
Al-Garadi *et al.* [75]	2018	Layer-wise security threats	Various ML and DL based countermeasures.	Yes
Saranyaa *et al.* [76], Hindy *et al.* [77]	2020	Considered IDS to identify and classify the security threats	Performance analysis of ML in IDS.	No
Aldweesh *et al.* [78]	2020	Analyzed IDS security	DL based countermeasures.	Yes
Chaabouni *et al.* [79]	2019	Surveyed on IDS security	ML and encryption based algorithms.	Yes
Costa *et al.* [80]	2019	Surveyed on IDS security	ML based countermeasures.	Yes
Moustafa *et al.* [81]	2019	Network layer anomaly detection	Decision algorithms including ensemble and DL	Yes

ware attacks and privacy leakage . In addition, the authors identify three major barriers to the potential implementation of shallow ML: processing and overhead distribution, security, and partial data learning techniques.

Whereas, Tahsien et al. [68] analyzed passive and active assaults based on IoT-layered architecture attack surfaces. The research examined various shallow ML algorithms along with the performance accuracy and expose the challenges to implementation. However, Zeadally and Tsikerdekis [69] reviewed IoT device properties and some common attacks. Authors also classified host-based and network-based security solutions using supervised, unsupervised learning techniques as well as addressed the necessity of existing ML methods improvement to adopt the constrained IoT environment. Gupta et al. [70] presented an extensive study of categorizing IoT attacks as goal, performer, and layered where DoS, MITM and selective forwarding attacks are addressed as critical IoT attack. In addition, ML-based solutions reviewed the complexity of the comparative algorithms and demonstrated that SVM was less complex than Neural Network (NN), although resource-constrained IoT networks posed enormous challenges. Hasan et al. [71] presented a most frequently observed IoT attacks and anomalies such as DoS, data type probing, malicious Control / Operation , scan, spying and wrong Setup. Authors also showed a comparative analysis of SVM, Logistic Regression (LR), DT, RF, and Artificial Neural Network (ANN) results in terms of precision, accuracy, recall, and f1 score to predict the considered attacks using virtual environmental dataset and showed that RF provides better performance than others. As the environment was virtually setup to collect the training dataset, authors recommended more robust algorithm which could handle real-time IoT frameworks. Amiri-Zarandi et al. [72] analyzed various data sources by introducing three layers of IoT paradigm, such as Application, Network, and Perception, and explained how to use different ML techniques to maintain privacy by optimizing data resources. Then, existing research gap was addressed to provide future work direction. However, Mamdouh et al. [73] provided a high level classification of IoT and WSN based frequent security attacks that is divided into three types; goal oriented, performer oriented, and layer oriented. Supervised (KNN, SVM, NN, Bayesian), unsupervised (principal component analysis, K-means clustering) shallow ML and reinforcement (Q-learning) was considered to counter various attacks specially DoS, selective forwarding attacks, MITM attacks etc.

Hussain et al. [74] provided an unique classification of security attacks that consists physical, network, transport, application, and encryption attacks. The work also reviewed ML and DL based solutions to overcome challenges of traditional cryptography by studying the various attack vectors and safety requirements. However, collecting datasets to ensure the unbiased outcomes of ML/DL algorithms is still a difficult task and novel hybrid methods are required along with various dynamic parameters to improve computational complexity, data driven technologies and learning efficiency. Al-Garadi et al. [75] provided a systematic study of layer-wise security threats and possible countermeasures based on ML/DL techniques. Various ML/DL methods are compared in terms of their advantages, disadvantages and area of implementation in IoT environment and find some extensive challenges that need to be solved to get better performance.

Nevertheless, Saranyaa et al. [76] presented a comparative analysis focused on common domain areas of various ML approaches (such as Linear Discriminant Analysis (LDA), Classification and Regression Trees (CART) and RF) in IDS. An ML-based experiment was also conducted using the KDD'99 cup dataset for IoT applications. The result showed that ML output depends on both the algorithm itself and the application field. Hindy et al. [77] presented IDS to detect attacks in MQTT using ML techniques such as SVM (RBF kernel), SVM (Linear kernel), LR, KNN, DT, RF, and NB. Also, a new IoT-MQTT dataset was developed to evaluate the performance of considered algorithms in terms of accuracy rate by addressing uni/bi-directional flow and packet-based IDS building features. Aldweesh et al. [78] surveyed in-depth learning security solutions for IDS and used a unique fine-grained classification based on input data, deployments, performance measurement strategies, and various designs. Authors suggested considering current datasets like CICIDS2017 and also demanded hybrid DL models like Generative Adversarial Network to boost DL algorithm performance. Chaabouni et al. [79] surveyed IDS in terms of state-of-the-art encryption techniques (such as central and distributed Snort, Suricata, Bro-IDS, Kismet, Sagan) and compared them with ML approaches such as MLP, Artificial Immune System (AIS), Supervised and Unsupervised Optimum Path Forest (OPF), ELM-based Semi-supervised Fuzzy C-Means (ESFCM). The performance evaluation reveals that the IDS using ML methods outperform other state-of-the-art methods. Costa et al. [80] studied more than 95 articles to understand IDS based on ML, such as SVM, Least-squares support-vector machine (LS-SVM), KNN etc.

Moustafa et al. [81] have reviewed ML-based network layer anomaly detection systems to impede the most common network threats by explaining cyber kill chain models and cyber-attacks. Additionally, NSL-KDD and UNSW-NB15 datasets are employed to present an experimental result for evaluating the decision algorithms including ensemble and DL in various applications like IoT, fog, and cloud computing.

Table 1 represents the addressed issues / contents and considered security solutions of IoT networks in existing review works.

III. IOT MODEL AND SECURITY CHALLENGES

Although no standardization of IoT architecture is defined, the TCP layer functionality is utilized to specify the operation, this section discussed IoT layers and protocols for each layer. Fig. 3 shows the five layer IoT architecture, these are– perception layer, network layer, transport layer, processing layer and application layer.

A. IOT MODEL

a: Perception Layer

Perception layer, also called sensor layer, is responsible for collecting information from sensor nodes and forwarding the collected information to the upper layer via an intelligent embedding controller. This layer includes different types of communication protocols such as Ethernet, IEEE802 families Programmable logic controller (PLC), Wireless Sensor Network (WSN), Global Positioning System (GPS), Near-Field Communication (NFC), Wireless-Highway Addressable Remote Transducer Protocol (Wireless-HART), Radio-Frequency Identification (RFID) Long Range Protocol (LoRa), Integrated Services Digital Network (ISDN), Bluetooth, Enterprise Service BUS (ESB), Integrated Development Environment (IDE), Digital Subscriber Line (DSL) etc. [82], [83], [84], [85]. A communication protocol can be chosen for a node based on the Quality of Service (QoS) demand.

b: Network Layer

Network layer is responsible for collecting processed information from the layer of perception and forwarding data to end-users or intermediate network devices, by choosing a unique path. For this layer, security requirements are highly anticipated as huge numbers of cryptography algorithms like RSA, ECC are used. This layer includes various technologies such as WSN, optical fiber communication networks, telephone networks, which is another reason to face various attacks. The most common network layer protocols are Internet Protocol version 4 and 6 (IPV4, IPV6), Internet Protocol Security (IPSec), Delivery Duty Paid (DDP), Enhanced Interior Gateway Routing Protocol (EIGRP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Open Shortest Path First (OSPF), Routing Over Low power and Lossy (ROLL), Routing Protocol for Low-Power (RPL), and Lightweight On-demand Ad hoc Distance-vector routing protocol-next generation (LOADng) [86], [87], [88].

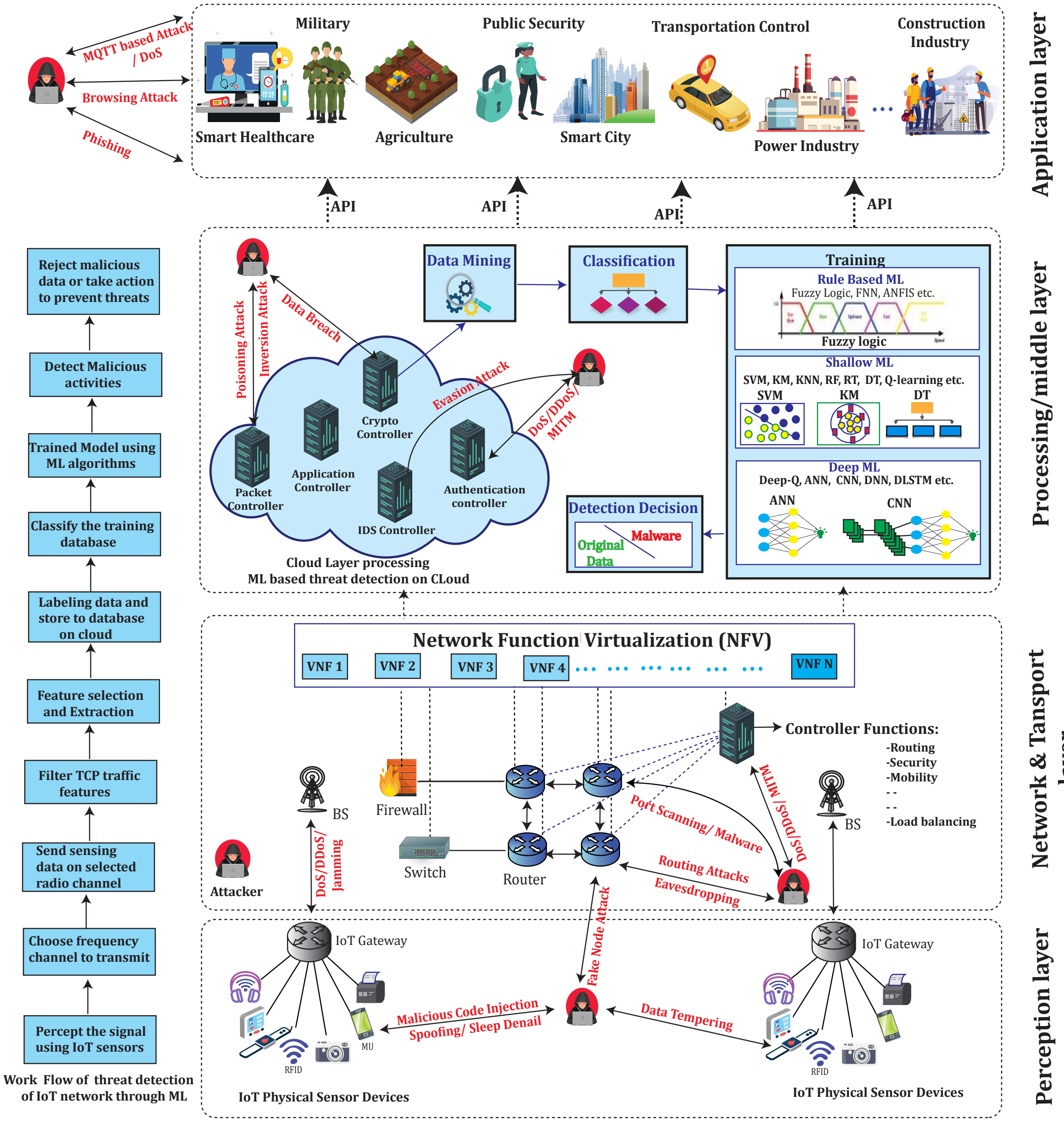

FIGURE 3. IoT architecture. Data captured by sensors in perception layer can be sent Network and Transport layer for reliable communication. Processing layer is responsible to secure Big data in cloud server where AI-based security mechanisms are implemented to provide security services to the Application layer users against frequent threats on IoT networks.

c: Transport Layer

This layer processed the incoming data from network layer and setup communication connection using UDP or TCP, retransmission, message error handling, access control. Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Quick UDP Internet Connections (QUIC), Datagram Congestion Control Protocol(DCCP), Stream Control Transmission Protocol(SCTP), and Real-Time Transport Protocol (RTP) are the popular protocols of this layer [89], [90].

d: Processing Layer

Processing layer (or middle layer) is responsible for collecting processed information from the transport layer, then providing the necessary services using the protocols specified, and then transferring the information to the upper layer. This layer includes many technologies including data servers, fog networks, cloud computing, and big data analysis. This layer provides end-user contact protection.

e: Application Layer

Application layer, also known as the business layer, is the topmost layer in the layer architecture of IoT. As IoT is used on the different platform, this layer is adaptable and configured to meet user requirements and industry specifications. User authentication, entry, message-oriented services, user interfaces are the layer's most common services. Message

Queue Telemetry Transport (MQTT) , Constrained Application Protocol (CoAP), Data Distribution Service (DDS), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), Representational state transfer (REST), Hyper Text Transfer Protocol (HTTP) are responsible for the application layer [89], [90], [91]. Recently, each IoT network has application and user interfaces, making protection more difficult than before.

Table 2 listed the above five layers IoT network's protocols and corresponding threats.

B. SECURITY CHALLENGES

Confidentiality, source authentication, and availability are considered essential security criteria in IoT networks where data freshness, stable system localization, time synchronization, and self-organization are addressed as minor [11]. However, it is also more challenging to maintain personal data protection, user authentication, threats handling, encryption, access control, network security , application security, restricted resources devices and latency in IoT network architecture [92]–[94].

IV. SECURITY THREATS

IoT transforms our way of life, makes us more productive and facilitates our lives. However, IoT systems are susceptible to unknown and unprecedented threats which can lead to compromised systems. This segment addresses layer-wise current threats based on presented architecture.

A. PERCEPTION LAYER THREATS

The perception layer is designed to generate and collect data via sensor/detection nodes. The data can then be transmitted through the hub/gateway nodes. In this layer, the wireline communication protocol includes IEEE 802.3 (Ethernet), power line communication (PLC), and Digital subscriber line (DSL) whereas the wireless protocols used in this layer includes, IEEE 802.11 series, 802.15 series, RFID, NFC, Integrated Services Digital Network (ISDN), Wireless-Highway Addressable Remote Transducer (HART), LoRa. The most frequently reported perception layer are Jamming, Spoofing, Sleep denial, Fake node, and Data tempering.

Jamming is a well-known threat that becomes an inevitable issue for IoT networks. In such attack, an attacker stealthily jams the network to make a channel occupied unnecessary among different nodes and hampered legitimate communication by creating node availability problems. Upadhyaya et al. [97] addressed intermittent jamming attacks where the adversary events have occupied the network for various intervals and sleep when even not want to jams the network to increase the transmission delay and reduce throughput of the network. Gwon et al. [98] provided a mathematical jammer formula to create jamming attack. It also discussed various types of jammers based on the way of jamming the authorized channel. For instance, Constant jammer sends random waveforms continuously; deceptive jammer adds the noise with legitimate packets; reactive jammer stays silent in a channel to transmit noise whenever sense any activity; strategic jammer is more intelligent to adapt anti-jamming procedures and causes more damages. On the other hand, Aref et al. [99] addressed the jamming problem for wideband autonomous cognitive radios (WACRs) where the attacker attempts to insert a jamming signal in the ongoing transmission of a secondary user to reduce the spectrum utilization through strategic jamming.

Spoofing is a frequent threat in IoT networks that is initiated by an attacker with the false broadcast messages which are sent by the spoofed Mac addresses or RFID tags. The original networks assume that the message is authentic and accept it falsely. This scenario is the most common to make a system vulnerable and causes authenticity, integrity, and confidentiality risk. Xiao et al. [100], [101] proposed a zero-sum authentication game where the receiver and spoofing attacker modeled based on Bayesian risk over universal software radio peripherals (USRP). Shi et al. [102] analyzed a spoofing attack in existing WiFi signals produced by indoor IoT devices to detect the uniqueness of human activity and WiFi fingerprints. However, Hamza et al. [103] addressed ARP spoofing that was employed over a smart home IoT environment.

Since IoT networks deal with low power sensor devices, they perform their functionality by replacing batteries or using power management (using active-idle-sleep cycle) to improve the lifetime of the batteries. A cyber attacker can launch a sleep denial attack to modify the usual sleep routine or force to be awake by keeping the targeted node busy and losing the battery power. Often, attackers can turn off the targeted devices. Hei et al. [104] analyzed resource depletion attack, which is launched by a simulation tool, called software Radios, in Implantable Medical Devices (IMDs) that have been used to treat chronic diseases. A patient can be harmed directly by this attack or reduce the battery life of an IMD.

Fake node attack occurs when an attacker adds a fake physical communication node between two legitimate nodes to inject malicious information or take control over data flow. Khatun et al. [105] used a threat model to evaluate the efficiency of the multi-layer ANN classifier by using smart bulbs that were connected to the mesh topology via WiFi network and generated modified real-time attack vectors. However, Meidan et al. [106] setup an attack model using malicious nodes to collect various features, including time-to-live of TCP packets to evaluate the proposed unauthorized node detection mechanism.

Data tampering attacks have frequently been launched in IoT to moderate, disrupt, or change confidential information through unauthorized networks. Goel et al. [107] proposed a DeepRing framework for the creation of a stable, efficient, versatile and scalable IoT distributed network. The authors considered the NIST and the CYPAR-10 datasets to construct a data tempering attack model.

TABLE 2. Layer-wise IoT protocols and Threats

Reference	IoT Layers	Protocols	Security Threats/attacks
[82], [83], [84], [85]	Perception	IEEE 802.3 (Ethernet), PLC, and DSL, IEEE 802.11 series, 802.15 series, RFID, NFC, ISDN, Wireless-HART, LoRa	Jamming, Spoofing, Sleep denial, Fake node, and Data tempering.
[86], [87], [88]	Network	IPV4, IPV6, IPSec, EIGRP, BGP, ICMP, OSPF, RPL	DoS/DDoS, Eavesdropping, Wormhole/Sinkhole/ Rank , Sybil , MITM , Local repair, Reply
[89], [90]	Transport	TCP, UDP, DCCP, SCTP, QUIC	port scanning, flooding, authorization, malware
[95], [96]	Processing	ML, data analytic and data predictive protocols	Fog based attack, virtual attack, code injection attack, data temper, Evasion attack, Poisoning attack, Inversion attack.
[89], [90], [91]	Application	MQTT, CoAP, DDS, XMPP, AMQP, HTTP, REST	Browser attack, Phishing, MQTT based, Malicious code injectionn

B. NETWORK LAYER THREATS

The network layer is responsible for providing a platform for communication among different networks. As a consequence, this layer is targeted by various attacks such as DDoS, Eavesdropping, Wormhole attack, Sinkhole attack, Rank attack, Sybil attack, MITM attack, Local repair attack, and Reply attack. IPV4, IPV6, IPSec, EIGRP, BGP, ICMP, OSPF, RPL, ROLL are the most common protocol of this layer.

Eavesdropping triggered when an attacker has access to a private conversation to make the device vulnerable by hacking a password or some data during transmission, which poses a high risk of confidentiality. Nguyen et al. [108] addressed the eavesdropping attack between switches where a hacker can insert fake Link Layer Discovery Protocol (LLDP) packets or send targeted LLDP packets to another switch to establish a false link between targeted switches and attacker switches. Sivaraman et al. [109] demonstrated threats to use of smart devices such as lamps, smoke detectors, or baby monitors. For example, smart bulb controls a home lighting system wirelessly where an Ethernet-enabled bridge accepts interface commands from the user and communicates them to the bulbs using the ZigBee-Light communication protocol. The eavesdropper may reduce the bulb functionality by exchanging data between the app and the bridge through HTTP commands.

DoS / DDoS is a related form of network layer attack. DoS attacks occur when a hacker uses a host to transmit overwhelming messages to a target device or server, resulting in the system being shut down so that authorized users are unable to access them. Unlike DoS, DDoS uses several hosts to attack the target device. Doshi et al. [110] created a DoS attack vector on the smart home LAN where a malicious device can monitor network traffic to inspect, store, manipulate, and block the network traffic.

Various routing attacks, such as wormhole attack, Sinkhole attack, or Rank attack, have been carried out to make IoT networks vulnerable. In a wormhole attack, the attacker maliciously formulates a wired or wireless link known as a tunnel to forward the transmitted packet faster than the normal routes. In the network layer, the attackers often referred to a less optimized route by changing the optimized route rank using rank attack. However, in sinkhole attack, a malicious user adds a sinkhole node that is an enticing and optimal route so that the network traffic goes forward. Shukla [111], Zahra et al. [112] and Bostani et al. [113] have formulated a wormhole threat model in the WSN or RPL network that can generate a terrible result, including network alteration, falsification or node manipulation. However, Napiah et al. [114] generated a hello flood, sinkhole attack and wormhole attack vector periodically using the Cooja simulator to test the performance of a ML based IDS algorithm for the 6LoWPAN network.

In the Sybil attack, a single unauthorized device claims a number of identities that are considered an unequal allocation of resources by the sybil device. Singh et al. [115] considered a sybil threat model where a malicious node joins the network using a single spoofed identity to reduce network performance. Wang et al. [116] used Renren (Chinese social network with nearly 220 million users) dataset to model the sybil attack vector to test the performance of the proposed security model.

In IoT architecture, hello flood attack is commonly taking place in the network layer. An adversary node sends an enormous hello request to a legitimate node using high transmission power and renders the node inaccessible to the authorized user [114].

Another routing attack, called Local Repair Attack, which is used in the RPL protocol when IoT devices are connected to IPV6. RPL-based network topology requires continuous updates on new node insertion, deletion, streaming of optimized rank information, etc. In such instances, a local repair attack may be carried out by a malicious node that intermittently activates all of its nearest neighbors. However, there is no issue with dropping valid packets, generating control overhead, raising the delay for packet [117].

In a MITM attack, an attacker can eavesdrop or monitor the transmission between two IoT devices and breach the protection of the devices by obtaining private information. Alaiz-Moreton et al. [118] created MITM.csv dataset by establishing a communication link between a sensor and a broker in the laboratory setting and created 3855 attacked frame within 110668 frames using Kali Linux and Ettercap tool to capture the significant changes of the IoT network. However, Farris et al. [119] exhibited how the attacker changes wrong temperature values in targeted Building Automation System

(BAS) devices. However, Kiran et al. [120] build a threat model using Node MCU ESP8266, DHT11 sensor, a laptop, and wireless router to collect a test dataset for a MITM attack to measure the efficiency of various ML algorithms.

A Replay attacker may collect a signed packet and then sends it multiple times to the target to keep network busy unnecessarily. Ghadekar et al. [121] generated a reply attack in the smart home system that intercepted the communication between the IoT devices and gateway.

C. TRANSPORT LAYER THREATS

Transport layer refers various protocols to ensure authenticity, data integrity and security on a communication network. It also includes a mechanism for the delivery of communication. TCP, UDP, DCCP, SCTP, QUIC are the popular protocols of this layer. Flooding, unauthorized access, port scan, malware are most frequent reported threats on transport layer.

Flooding attacks are also known as a DoS attack, designed to cause mass transmission or traffic down to a communication channel or service. The UDP, Acknowledgement (ACK) flood, Domaine Name System (DNS) flood, and Synchronizing (SYN) flood attack vectors using the mirai botnet dataset have been analyzed by McDermott et al. [122] to build DDoS on IoT networks. By generating a wide variety of packets with random MAC and IP addresses to cause floods on switches flow table or create a DoS attack, Liu et al. [123] and Bull et al. [124] planned a flood attack against the SDN controller. Bhunia et al. [149] showed the detection of TCP/ICMP flooding attack in IoT devices through a blacklisted IP source address in the SDN-based SoftThings platform.

A malicious user may access confidential information or gain ownership of data through unauthorized access. The access control can prevent the entry of unauthorized users to the IoT devices. Li et al. [125] developed a cyber-attack model to login to the target IoT system to test the performance of the proposed access control process. Nobakht et al. [126] stated the vulnerability of unencrypted communication between the smart light app and the local bridge, and created a python script to initiate an attack to take control of the smart light by interrupting network traffic or generating commands as a legitimate user.

A client request is sent to a number of server port addresses by an attacker via Port Scan Attack to detect an active port and its exploitable service vulnerability. In order to detect port vulnerability by sending an unauthorized request, Li et al. [125] designed a port attack model using the Nmap tool.

Malware or malicious software introduced into a network to infect cloud/data servers. Nguyen et al. [127] developed an attack model using a Mirai malware sample that is launched into a weak Small office / Home Office (SOHO) network to investigate the efficiency of the proposed attack detection model. Su et al. [128] used IoTPOT to collect threat samples from different malware families such as Mirai and Linux.Gafgyt then passes malware samples to malware gray scale images to identify the malicious behavior of the IoT network. However, Feng et al. [129] have used Fake Installer and DroidKungFu malware sample families found in android repackaging. Gu et al. [130] have developed a fuzzy multi-feature model using different Android-based malware samples to test the performance of the suggested blockchain-based malware detection framework.

D. PROCESSING LAYER THREATS

Processing layer or middle layer comprises a range of technologies such as cloud computing, fog computing, database, big data analysis, etc. The ML based data analytics protocols, therefore, provide enormous services for this layer. The most frequently launched attacks are Fog based attacks, Code injection attacks, Virtual attacks, Evasion attacks, Poisoning attacks, and Inversion attacks.

Due to heterogeneous IoT topologies and smart artifacts, fog attackers can easily launch multiple threats. DDoS, MITM attack, flooding, etc. are familiar node-based attack. Alrashdi et al. [131] examined fog-based attacks like jamming, DDoS, Sybil, etc. on proposed IoT healthcare architecture that adversely inhibits fog node operation. Abeshu and Chilamkurti [132] addressed the impact of ransomware malware, fake ICMP flooding, and DDoS attack on small fog nodes capable of blocking data, reducing transmission rate, or crashing the fog system.

In IoT cloud environment, Code injection attack occurs when the web application receives malicious data and processes it without recognizing the harmfulness. SQL injection, shell command injection, operation system injection, etc. are common types of code injection attacks that make a system vulnerable. Therefore, providing data confidentiality, integrity, and authentication for web applications is getting challenging. Ogbomon et al. [133] employed numerical attributes extraction from NETSQLIA dataset to evaluate the SQL Injection Attacks in IoT cloud devices.

Virtualization in the cloud allows users to use underlying hardware from abstract resources. Attackers exploited virtualization technology for malicious behavior. Attackers could jeopardize virtual machine (VM) infrastructures, enabling them to access other VMs on the same device and host. The virtual attack is one of the most potential threats where an attacker acts toward a virtual machine to steal sensitive information or gain control of the system for various malicious reasons. Chung et al. [134] developed an attack graph model to demonstrate all possible attack routes in a network that helps assess and classify potential internal and external vulnerable virtual machine attacks. Besides, Zhou et al. [135] addressed unauthorized users who can copy, alter, leak, or use important confidential data through breach activities.

The ML approaches have a great implementation area on a IoT network such as threat detection, spectrum management, resource allocation, traffic management, and data retrieval. However, an attacker can also attempt malicious activity amid the test time of an ML algorithm to influence the attack samples, known as evasion attack. The main vision

TABLE 3. Brief description of Layer-wise IoT network threats

Reference	IoT Layers	Threat/Attacks	Description
[97], [98], [99]	Perception Layer	Jamming	Creates noise signals in same transmission frequency.
[100], [101], [102]		Spoofing	Send unauthorized packets into network.
[104]		Sleep denial	Lose the power or alter the sleep routine of IoT devices.
[105]		Fake node	Unauthorized node is placed.
[107]		Data tempering	Destroy or alter sensitive information.
[110]	Network Layer	DoS and DDoS	Sends overwhelming messages to the network.
[108], [109]		Eavesdropping	Access private communication to steal information.
[111], [112] , [113], [114]		Wormhole/Sinkhole/ Rank	Modify packet routes, flow speed, rank of the nodes.
[115], [116]		Sybil	A single malicious node use multiple identities.
[114]		Hello flood	Sends hello request to makes a node unavailable.
[117]		Local Repair	Manipulate RPL-based networks status.
[118], [119], [120]		MITM	Eavesdrop and possibly changes the communication.
[121]		Reply	Resend signed packets multiple times.
[122], [123], [124]	Transport layer	Flooding	Create large number of traffic to down the network.
[125], [126]		unauthorized access	Get sensitive information by unauthorized access.
[125]		Port scanning	Find significant weakness on targeted system.
[127], [128], [129], [130]		Malware	Send malicious software to access sensitive data.
[131], [132]	Processing Layer	Fog based	Launch various threats in fog IoT nodes.
[133]		Code injection attack	Find significant weakness on targeted system.
[134], [135]		Virtual	Steal data or take control over a virtual machine.
[136], [137]		Evasion	Manipulate data during prediction stage of a ML algorithm.
[138]		Poisoning	Inject false training data into Ml algorithm.
[139], [96]		Inversion	Reveals confidential value along with the prediction.
[140], [141]	Application Layer	Browser based	Hampered or stealing the significant data.
[142], [143], [144]		Phishing	Send fake links, emails or messages to deceive.
[145]		MQTT based	Target MQTT protocol to reduce the data transfer performance.
[146], [147], [148]		Malicious code injection	Injects unauthorized code or data segment.

of an evasion attack is to manipulate the test data to produce the misclassification result [136]. Ibitoye et al. [137] experimented with an evasion attack during the DL-based IDS prediction process. The work considered the BoT-IoT database from the UNSW Canberra Cyber lab to get the faithful demonstration of IoT network.

Poisoning attacks occur when an intruder injects false training sample to an ML algorithm for taking a wrong decision. Sagduyu et al. [138] found that poisoning attacks would minimize DNN-based IDS predictability. Feedforward neural network was used as defensive mechanism which was implemented to systematically increase the adversary's confusion at the inference stage and enhance efficiency. The findings provide new insights into how IoT networks can be attacked and defended with high success rate.

Inversion attack is a new class of ML model attacks, which evasively used important data and revealed its importance in accordance with the prediction. Papernot et al. [139] analyzed an attack on the victim model during training on the opposite activity line reversion line. Two ML models, SVM and DT, demonstrated the attack for Google and Amazon platforms. However, during training faces, Fredrikson et al. [96] used the DT and NN inversion attack to minimize the prevision performance.

E. APPLICATION LAYER THREATS

Application or abstract layer specifies various communication protocols such as MQTT, CoAP, DDS, XMPP, AMQP, HTTP, REST in TCP/IP model. Browser attack, Phishing, MQTT based attacks, Malicious code injection are more common in application layer.

IoT has been implemented in many applications, but there is no standard for application construction yet, data sharing in the upper layer faces some threats including browser attacks. Using common web browsers like Mozilla Firefox, Google Chrome, or Microsoft Internet Explorer, attackers can access other devices to spread malicious information or steal sensitive network information. Liu et al. [140] tackled the cryptocurrency browser mining attack where the browser was blocked by malicious mining activities. Kumar and Lim [141] analyzed the Browser-based attack using HTTP, SOAP, PHP protocols in smart IoT networks.

Phishing has been introduced as a common way to deceive people using social engineering techniques through short messages, ads, or emails to search fake websites for accessing credential details such as bank accounts, credit card information, payment tokens, personal information, etc. Mao et al.. [142] and Yi et al. [143] mentioned a web-based phishing problems for mobile and IoT systems where attackers are prone to access authorized users sensitive information using fake websites link. Wu et al. [144] analyzed the effect of phishing attack between smart bulb mobile application and Nest server which launched to steal PIN code of the user.

MQTT is a significant application layer protocol that is used to send the information between IoT nodes. An attacker can also target the MQTT protocols information to reduce the performance of data transmission. Ciklabakkal et al. [145] analyzed the threats on MQTT broker in IoT environment to evaluate the functionalities of a proposed IDS system.

Malicious code injection attack initiates when an attacker injects an unwanted code or data segment into an application for network access and likely system vulnerability. Ferdowsi and Saad [150] proposed two types of malicious code injection attacks. In one form, the attacker adjusts the IoT device signal and in another form, the attacker collects the transfer data from IoT devices and then extracts the bit stream to prepare an attack using the same watermarking bits. Ozay et al. [147] used distributed and collaborative sparse attack vectors to create false code injection attacks in electrical grids where the attacker would easily access the power system to change meter information for random errors. On the other hand, Azmoodeh et al. [146] initiated the junk OpCode insertion attack created using malware samples from the VirusTotal2 platform to cause severe IoT network loss. However, Alves et al. [148] studied the open existence of Modbus and DNP3 protocols that produce an injection attack on the water storage tank SCADA device in the real open source Programmable Logic Controller (OpenPLC).

Table 3 represents the brief description of above discussed layer wise IoT networks common threats and their effects.

V. AI BASED SECURITY SOLUTION

A lot of research has been conducted to enhance IoT network security by alleviating various attacks. This section provides the features of different ML and DL approaches that can accelerate the performance of security mechanisms for smart IoT networks. We have divided the traditional ML approaches into two categories. One is rule-based ML and another is shallow ML. Rule-based ML methods are required a set of pre-defined protocols to design the model and manipulate the trained data automatically based on the given actions. Among various rule-based ML techniques, FL, Fuzzy Neural Network (FNN), Neuro-Fuzzy Inference System (NFIS), etc., are more popular. On the other hand, in shallow ML techniques, the process of feature extraction requires domain knowledge of the information that the model is learning from. Algorithms of shallow ML depends on their area of implementations and the pattern of the prediction which are categorized as regression, classification, clustering, and reinforcement learning. DT, SVM, NB, KNN, RF, Ensemble Learning, etc., are popular shallow ML methods that are use to classify or cluster the train data to detect malicious activity in the network.

However, nowadays, researchers are more interested in DL approaches rather than traditional ML methods. DL utilizes a hierarchical structure of multiple layers of ANN which use sophisticated mathematical solution through algorithmic computation and are often outperformed compare to the traditional (shallow) ML techniques. DL also able to extract features automatically using multiple layers of processing from original data with slight or without preprocessing. Among immense applications of DL models, ANN, CNN, RNN, Autoencoder, etc., are more prominent to handle various threats in IoT networks.

A brief overview of the various ML / DL approaches is given in the table 4. Moreover, fig. 4 represents the classification of various AI based countermeasures in IoT security which are considered in this paper.

The Layerwise AI/ML based security threats countermeasures are discussed more details below:

A. PERCEPTION LAYER THREATS COUNTERMEASURE

The jamming attack has a thoughtful impact on IoT devices. Gaussian SVM, K Nearest Neighbor, Random Forest, and REP Tree were used to detect a signal jam-attack by Upadhyaya et al. [97]. The author considered five dedicated nodes for evaluating the performance of real Network data using the Received Signal Strength Indication (RSSI) dataset. Moreover, testing the accuracy of 89.7% and 99.01% were achieved for single and multiple path channels. Gwon et al. [98] proposed an anti-jamming architecture using Q-learning-based reinforcement techniques and showed that Minimax-Q is more appropriate compared to Nash-Q for a mobile network game. Mohamed A. Aref et al. [99] considered Multi-Agent Reinforcement learning-based sub-band selection framework for anti-jamming using Q-learning for WACRs. However, for improving the performance of [99], Guoan Han et al. [151] used Deep Q-learning based solution and saved almost 66.7% time compared to Q-learning.

Many researchers used learning algorithms and improved protection in contrast to conventional cryptography to counter the spoofing assault. Xiao et al. [100] employed a Q-learning algorithm for physical layer authentication using RSSI data. To achieve the optimal threshold for spoofing detection, Bayesian risk-based PHY-authentication game approach is considered between the link of a valid receiver node

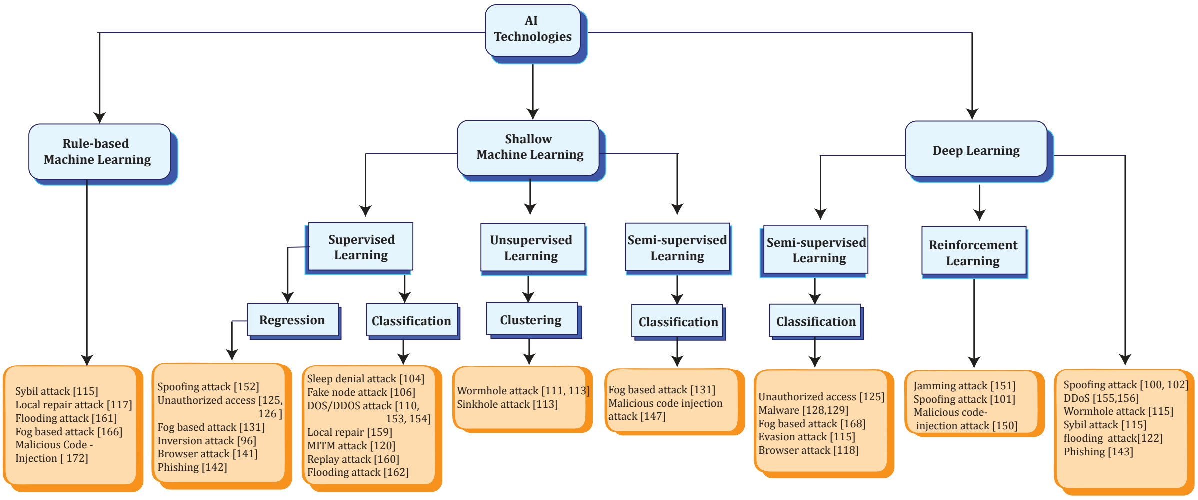

FIGURE 4. Classification of Machine Learning Techniques used for the countermeasures of various types of IoT attacks.

and a spoofer through USRP. For the same environment, Xiao et al. [101] used Deep-Q and Dyna-Q based reinforcement learning algorithms to spoofing attack on the physical layer and provide secure authentication with less error. Another work of xiao et al. [152] used supervised Incremental Aggregated Gradient (IAG) learning techniques for physical layer protection and reduce overhead against spoofing related threats. Shi et al. [102] have proposed DNN based advanced authentication system. The author utilized the device-free mechanism and achieved 92.34% accuracy by mining CSI features of the WiFi signals.

Resource scarcity is one of the sleep denial attack's rudimentary factors. Hei et al.. [104] introduced an SVM-based authentication scheme to protect medical devices from resource depletion. The simulation result showed that the detection accuracy of the SVM classifier exceeds 90%.

Instead of detecting malicious activities, Akhi et al. [105] focused on detecting the fake IoT nodes for network security. The work suggested an ANN-based mechanism to train a modified real-time traffic dataset, which was captured using pcapng format from smart bulbs to identify the fake node and showed high accuracy. Meidan et al. [106] proposed a multiclass classifier by combining RF and DT algorithms to identify the malicious nodes in IoT environment. The work considered 17 different IoT devices to capture the data and showed 99.49% accuracy rate for 110 consecutive sessions for other locations. The perception layer security countermeasures are presented in table 5.

B. NETWORK LAYER THREATS COUNTERMEASURE

Increased connectivity of heterogeneous IoT nodes with limited resources makes DDoS attack for making a node vulnerable by implementing invalid request flooding. Doshi et al. [110] proposed anomaly detection techniques using KN, LSVM, DT, RF, deep NN binary classification to detect Distributed DoS with accuracy rate from 91% to 99%. An experiment was set up for getting a real-time dataset using a middlebox (Raspberry Pi V3 WiFi access point), Home camera, smart switch, blood pressure monitoring, and android application. The result also showed that home gateway devices and other network middleboxes could be an effective way to detect the attack with less cost automatically. Kozik et al. [153] employed Extreme Learning Machine (ELM) classifier to detect DoS attack in cloud environment. Mehmood et al. [154] deployed multi-agent-based IDS to detect and prevent the DDoS attack, which used naïve Bayes classification methods to train the NSL-KDD dataset. However, Roopak et al. [155] trained 1d-CNN, MLP, LSTM and CNN+LSTM DL algorithms using updated CICIDS2017 dataset. The result showed that the CNN+LSTM classifier performs better than others with a 97.16% accuracy rate. The author also compared the DL algorithms with the existing typical ML algorithm and got an improved result. On the other hand, Meidan et al. [156] proposed self-learning based deep autoencoders for botnet detection by considering Mirai and BASHLITE attack vectors.

Xiao et al. [101], [157] proposed Q-learning and IGMM Nonparametic Bayesian authentication techniques to detect the eavesdropping which is used to classify RSSI data for wireless sensing environment. In [157], proximity-based security is employed where each client has a unique private session key (Secret location tag) to resist eavesdropping activity.

Shukla et al. [111] suggested three intrusion detection system for detecting wormhole attack in IoT. The author considered centralized unsupervised K-means clustering and supervised decision tree to detect the wormhole attack with 70-93% and 71-80% detection rate respectively by presenting

TABLE 4. Artificial Intelligence techniques for threat countermeasure

Type	Algorithm	Description
Rule based	FL	FL provides a set of rules to govern a decision for making a system based on linguistic information.
	FNN/ANFIS	FNN / Adaptive Neuro-fuzzy inference system (ANFIS) utilizes fuzzy protocols with the combination of neural network.
Shallow ML	SVM	SVM creates splitting hyperplane among various class data to classify the given samples.
	KNN	Classifies data or device characteristics in terms of malicious activity based on the nominated nearest neighbor's votes.
	RF	Tree based Supervised ensemble learning model which construct a multitude of DT to predict the output.
	DT	Supervised predictive model which uses a decision tree to observe and reach in the conclusion.
	NB	Find the posterior probability of an event based on the given information to classify the abnormality of a network.
	Q-learning	Utilizes off policy learning algorithms to maximize the total reward through considering random action.
	IAG	IAG considered previous gradient values in memory and process the functions in a deterministic order.
	EL	Ensemble Learning (EL) combines multiple base ML models to provide better prediction performance.
DL	MLP	MLP utilizes back-propagation for training with the help of hidden layer
	CNN	Reduces the connection between layers and combines convolutional layer with pooling layer to deteriorate training complexity.
	RNN	Works on graph-like structure to detect malicious data in time-series based threats
	DNN	DNN processes the supplied data to recognize the pattern or predict the desired result more globally through multistep.
	LSTM	LSTM is a feedforward NN that is able to process a sequence of information apart of a single data.
	DQN	Combines the concept of traditional Q-learning along with the deep neural network to enhance the performance of Q function.
	GRU	Gated Recurrent Unit (GRU) algorithm is an alternative of LSTM but faster because of not having the exposure controlling mechanism to which sample flow is submitted.
	AE	Auto-Encoder (AE) use to feature extraction without considering prior knowledge.

TABLE 5. Perception layer Threat/Attack countermeasures

Threat/Attacks	ML types	Countermeasure techniques	Ref.
Jamming	Shallow ML	SVM, KNN, RF, RT	[97]
		Q-Learning	[98], [99]
	DL	DQN	[151]
Spoofing	Shallow ML	Q-learning	[100]
		IAG	[152]
	DL	DQN	[101]
		DNN	[102]
Sleep denial	Shallow ML	SVM	[104]
Fake node	DL	Multi-layer ANN	[105]
	Shallow ML	RF, DT	[106]

a safe zone and safe distance among neighboring routers. This paper also introduced distributed two-stage hybrid lightweight ML-IDS by combining K-means clustering and Decision tree that provide 71-75% detection rate but with more accuracy than others. Zahra et al. [112] have proposed a wormhole detection framework using a ML approach. The paper only considered Routing protocol attacks by analyzing the security features of RPL and differentiating the valid and invalid nodes in case of wormhole attacks. Bostani et al. [113] designed a novel anomaly-based IDS system using an unsupervised optimum-path forest algorithm to detect Sinkhole and wormhole attack with 76.19% and 96.02% true positive rate, respectively. The author employed the MapReduce paradigm to project the clustering model and detect the anomalous events using a detection specification-based agent located in router nodes. Singh et al. [115] introduced Advanced hybrid IDS based on Multilayer Perceptron Neural Network (MPNN) where the combination of Backpropagation and Forward Neural Network is used to detect wormhole attack and hello flood with 99.20% and 98.20% detection rate respectively.

Singh et al. [115] proposed advanced hybrid IDS using the FL and MPNN to identify malicious nodes and various types of attackers such as Sybil attack, wormhole attack, and hello flood attack. The Hello flood attack was detected using RSSI and distance. In a node sets analysis, 13.33 % of nodes were determined as misbehaving nodes, which categorized attackers. The system detected Sybil, hello flood, and wormhole attacks with high accuracy (0.994 vs 0.982 vs 0.992).

Farzaneh et al. [117] proposed a fuzzy-based new IDS system for detecting the local repair attack on IPV6-RPL routing protocols. The work considered distance, residual energy, and expected transmission count metrics to demonstrate the fuzzy composition and showed a high accuracy rate using the Cooja simulator. Verma and Ranga [159] introduced ELNIDS, which used EL-based classification to train the NIDDS17 dataset against IPV6 routing protocols to detect various routing attacks, including local repair attack, sinkhole, Sybil, and hello flooding.

Alaiz-Moreton et al. [118] employed three different ML approaches such as GRU RNN, Extreme Gradient Boosting, and LSTM-RNN mechanisms to train the moderated dataset for impeding the other type of attacks, including MITM attack. The result showed that the selected classification methods are efficient in GPU implementation, and the per-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3089681, IEEE Access

TABLE 6. Networklayer Threat/Attack countermeasures

Threat/Attacks	ML types	Countermeasure	References
DoS/DDoS	Shallow ML	KN, LSVM, DT, RF	[110]
		ELM	[153]
		NB	[154]
	DL	4–layer NN	[110]
		CNN, MLP, LSTM, C-LSTM	[155]
		Deep AE	[156]
Eavesdropping	Shallow ML	Q-learning	[101]
		IGMM-NB	[101], [157]
Routing	Shallow ML	KM, DT, HKM	[111]
		OPF	[113]
		MLP, J48, NB, RF, SVM	[114]
		NB	[158]
		EL	[159]
	DL	MLP NN	[115]
		MLP	[158]
Sybil	Rule based	FL	[115]
	Shallow ML	SVM	[116]
		EL	[159]
Local Repair	Rule based	FL	[117]
	Shallow ML	EL	[159]
Hello Flood	Shallow ML	J48, NB, RF, SVM	[114]
		EL	[159]
	DL	MLP	[114]
		MLP NN	[115]
MITM	Shallow ML	NB, SVM, DT, Adaboost	[120]
	DL	GRU RNN, EGB, LSTM-RNN	[118]
Replay	Shallow ML	NB, J48, SVM, Zero/one-R, RF	[160]
	DL	MLP	[160]

Legend: HKM– Hybrid KM; IGMM-NB– IGMM Nonparametic Bayesian; C-LSTM–CNN+LSTM; Routing–Sinkhole/Rank/Wormhole;

formance of ensemble learning is better than deep and linear learning methods. Kirana et al. [120] build an IDS using various ML classification algorithms like NB, SVM, DT, Adaboost to detect MITM attack, which was performed in the proposed network through ARP poisoning. The work recommended a high-quality training dataset for getting the better performance of ML algorithms.

Anthi et al. [160] proposed a three-layer IDS architecture supervised novel against some common network layer assault, such as MITM attack, replay attack, and DoS. The system's key functions were distinguishing regular and malicious packets, including the attack name for smart home IoT products. NB, Bayesian Network, J48, SVM, Zero R, OneR, MLP, and RF are used to classify the training dataset generated using Weka software, showing J48 to be the most powerful.The network layer AI based security mechanisms are listed in table 6.

TABLE 7. Transport layer Threat/Attack countermeasures

Threat/Attacks	ML types	Countermeasure	Ref.
Flooding	Rule based	Neuro Multifuzzy	[161]
	Shallow ML	Linear/Non–linear SVM	[162]
	DL	RNN	[122]
Unauthorised Access	DL	RNN, NN	[125]
	Shallow ML	SVM	[126]
		LSTM	[163]
Port scanning attack	DL	RNN, NN	[125]
Malware	Shallow ML	Federated learning	[127]
		EL	[102]
		MICS	[164]
	DL	CNN	[128]
		Autonomous DL	[129]

C. TRANSPORT LAYER THREATS COUNTERMEASURE

IoT network requires secure data transmission. To secure data in the transport layer, Pourvahab and Ekbatanifard [161] proposed a forensic paradigm in SDN-IoT network which used Neuro Multifuzzy classification algorithm to identify the flooding attacks in the various port of the IoT devices. However, McDermott et al. [122] have designed a novel Bidirectional Long Short Term Memory based Recurrent Neural Network (BLSTM-RNN) for botnet detection using Mirai dataset. The author compared BLSTM-RNN and unidirectional LSTM-RNN in terms of accuracy and loss, where BLSTM-RNN was found as a better performer. Sankar et al. [162] have designed SDN based dynamic attack detection framework called SoftThings in IoT networks. Linear and Non-linear SVM classifier is used in SDN controller to detect and mitigate the TCP/ ICMP flooding and DDoS attack with 98% precision.

Li et al. [125] proposed a statistical anomaly-based attack detection system for auto-sustainable IoT devices using time-series analysis. The work used RNN, NN, and linear regression learning algorithm to classify Linux / Unix system statistical data obtained by plug-ins. To measure frame output, unauthorized access attacks, port scan attacks, and TCP flood attack vectors were designed to find high-efficiency malicious actions. Nobakht et al. [126] used IoT-IDM, SDN-based intrusion detection, and mitigation systems where a case study is proposed to defend the home system against unauthorized access. Logistic regression and SVM were used to train and detect the attacked host. IoT-IDM works to avoid attacks after finding the infected host. Agrawal et al. [163], however, developed a continuous secure access control protocol using blockchain techniques where each legitimate IoT-Zone user's transfer is stored in the blockchain. A unique crypto-token is required for allowed data access provided using the LSTM prediction model.

Duc et al. [127] presented DIoT architecture, federated learning-based automated self-learning distributed malware detection framework. Security gateways use locally collected

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3089681, IEEE Access

TABLE 8. Processing layer Threat/Attack countermeasures

Threat/Attacks	ML types	Countermeasure	Ref.
Fog based	Rule based	ESFCM	[166]
	Shallow ML	EL	[131]
	DL	Distributed DL	[132]
		MLP	[167]
		RNN, MLP, E3ML	[122]
		DNN	[168]
Malicious Code injection	DL	ANN	[133]
	Shallow ML	SVM, NB, KNN	[167]
Data Tempering	DL	CNN	[107]
Evasive	Rule based	FNN, SNN	[137]
Poisoning	DL	DNN	[138]
Inversion	Sallow ML	DT	[96]

data to train federated learning-based models and then use it as a global model that improves accuracy with 95.6% detection rate. Su et al. [128] used a lightweight convolutional neural network-based image classification method to detect malware attack. The classifier is trained by one-channel gray-scale images extracted from malware binaries and helps to detect malware attacks with 94.0% accuracy. On the other hand, Naeem et al. [164] focused on malware image classification system (MICS) using for large-scale IoT environment. MICS translates the obtained suspect activities into a gray-scale image. Then, local and global malware functionalities were captured to get fine-grained classification with a 97.4% accuracy rate. To preserve the security on Android applications, Feng et al. [129] proposed EnDroid, a malware detection framework to trace advanced and dynamic malicious behavior like sensitive information leakage using ensemble learning algorithm which is trained by AndroZoo and Debrin datasets with 98.2% accuracy rate. BillahKarbab et al. [165] have designed a novel MalDozer framework based on autonomous DL classifier which used multiple datasets including Malgenome, Drebin , new MalDozer, and benign apps downloaded from Google Play to detect malware attack for Android application. As every year, mobile devices are facing nearly 40-50 million malware attacks, google has designed enormous tools to protect the user application as well as devices. Possible security countermeasures of transport layer's are listed in table 7.

D. PROCESSING LAYER THREATS COUNTERMEASURE

Many researchers suggest fog network instead of the cloud. There have been introducing dynamic and real-time fog-based attacks. Rathore and Park [166] focused on fog-based attack detection and proposed Extreme Learning Machine (ELM) based semi-supervised Fuzzy C-Means (ESFCM) technique. They used NSL-KDD dataset for training the pattern and get 86.53% accuracy rate in terms of distributed attack. However, Alrashdi et al. [131] proposed fog-based attack detection (FBAD) architecture which used an ensemble of online sequential extreme learning machine (EOS-ELM) classifier to train NSL-KDD dataset and find the abnormal behavior with to 98.19% accuracy rate. The result also showed that EOS-ELM's performance is better than traditional ELM and OS-ELM to preserve the security of IoT healthcare devices in smart cities. Abeshu et al. [132] employed novel distributed DL-based Intrusion detection system to detect fog-based attack using soft-max regression (SMR) classification in NSLKDD dataset. To detect the fog-based attack, a supervised multilayer perception-based IDS system is introduced by Khater et al. [167] which is trained using new generation system call ADFALD and ADFAWD datasets with 94% and 74% accuracy rate respectively. Shafi et al. [169] proposed an intrusion detection and prevention system using RNN, ADT, MLP, and E3ML learning-based classifier that is trained by UNSW-NB15 dataset. They also involved fog assisted SDN controller using OpenFlow protocols to detect the anomaly and prevent the distributed attack dynamically in the fog network. Another work of Rathore et al. [168] proposed a novel BlockSecIoTNet which is a decentralized attack detection framework using SDN and Blockchain in fog and edge computing where SDN is responsible for monitoring the traffic and blockchain provides distributed attack identification. They considered DNN-based classification in fog nodes to mitigate fog based attacks, TCP Flooding, and DDoS.

The IoT network's critical role is to protect classified information from its servers. Uwagbole et al. [133], for detecting code injection attack on a database cloud server, have used the NETSQLIA-based numerical NETSQLIA dataset for IoT System to train Two-Class Averaged Perceptron and Two-Class Logistic Regression (TCL RR) for the use of ANN and statistical ML algorithms respectively. However, Komiya et al. [170] focused on the effect of injecting malicious code in web applications. SVM, Naïve Bayes, and KNN are considered to train the dataset to find the SQL malicious codes on the cloud.

Goel et al. [107] utilized deep neural network to proposed DeepRing architecture for impeding the data tampering attack. The work combined CNN along with blockchain concept to ensure the data integrity. MNIST and CIFAR-10 datasets were considered to train and got 99.07% and 83.89% accuracy rate, respectively.

To detect the evasion attacks over ML techniques, Ibitoye et al. [137] used FNN and Self-normalizing Neural network (SNN) to classify the intrusion on various ML algorithms in IoT network. The work also compared the detection performance between FNN and SNN using BoT-IoT dataset and get better results for FNN in terms of multiple measurement metrics like correctness, precision, and recall. Conversely, SNN showed effective outcomes against adversarial samples from the given dataset.

Sagduyu et al. [138] considered various defense models against attacks on ML techniques such as poisoning attack and evasion attack. The work introduced a Stackelberg game approach to maximize the performance of the defense procedure over the FNN algorithm.

Fredrikson et al. [96] initiated a novel countermeasure against Inversion attack using security-aware DT that is a modified version of CART learning using FiveThirtyEight dataset.

Table 8 lists the processing layers threats countermeasure corresponding to various ML types.

E. APPLICATION LAYER THREAT COUNTERMEASURES

In the blockchain environment, secure transmission of cryptocurrency is essential. An attacker may introduce browser-based malicious attacks to gain the cryptocurrency illicitly. Therefore, Liu et al.. [140] analyzed browser-based attacks by analyzing browser silent mining features. Based on the RNN, this decentralized blockchain scheme differentiates the malicious activity from the browser's memory snapshot and stack dynamic code feature to detect the browser-based silent miner feasibly. Kumar et al. [141] designed a novel IoT security framework, EDIMA, to detect malicious activity on application layer protocols like TELNET, HTTP POST, and HTTP GET. Supervised NB, DT, SVM to train packet traffic features dataset and differentiate between authentic and malware traffic.

The hacker conducts numerous external attacks, such as phishing, to steal PIN code and cause serious data leakage. Mao et al. [142] suggested anti-phishing techniques using SVM, DT, AdaBoost and RF classifiers to train phishtank.com datasets. The classifier considered CSS layout features for testing page similarity that helps identify phishing pages. Yi et al. [143] implemented a website DL phishing detection model where original URL and website interaction features are considered to train the model. Then use the Deep Belief Networks (DBN) training model to verify ISP 's current IP errors with 90% true positive rate.

MQTT is a significant application layer protocol that helps to transport messages among IoT nodes. Sometimes various smart attacks take place on the particular protocols. Ciklabakkal et al. [145] designed ARTEMIS, an IDS to detect MQTT protocol attack in IoT network. The training dataset collects using DHT11 sensor and used several ML techniques like RF, K-Means, Isolation Forest (IF), etc. to detect the malicious request.

Malicious code injection can modify the information and reduce the performance of IoT nodes. Ferdowsi and Saad [150] proposed a novel watermarking framework using reinforcement learning based LSTM to detect malicious code injection of IoT devices (IoTDs) by capturing stochastic features of the generated signal. The IoT gateway used Fictitious Play (FP) learning for complete information (Knows all IoTD's action) and LSTM learning for incomplete information. However, lightweight mixed-strategy Nash equilibrium (MSNE) based game-theoretic approach is considered to increase IoT gateway's decision-making process. The result showed nearly 100% massage transmission reliability of the proposed framework under one-second attack detection delay. Ozay et al. [147] used supervised SVM and semi-supervised SVM ML to predict false data injection attacks in the smart grid. The simulation result indicates that supervised SVM is less robust than semi-supervised SVM in terms of the degree of sparsity of training data. However, Fang et al. [171] invented a unique lightweight AI enable security mechanism using SVM and online ML to ensure faster authentication by detecting the malicious data injection attacks in the IoT networks. Table 9 demonstrates application layer countermeasures for the specific types of IoT threats.

TABLE 9. Application layer Threat/Attack countermeasures

Threat/Attacks	ML types	Countermeasure	Ref.
Browser based	DL	RNN	[140]
	Shallow ML	NB, DT, SVM	[141]
Phishing	Shallow ML	SVM, DT, AdaBoost, RF	[142]
	DL	DBN	[143]
MQTT based	Shallow ML	RF, K-Means, IF	[145]
Malicious Code Injection	Shallow ML	KM	[148]
		SVM	[147]
	Rule based	FL	[172]
	DL	LSTM	[150]
	DL	Deep–Eigenspace	[146]

VI. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Detection of security threats in IoT networks and corresponding counter measures are confronted with serious difficulties because of the lack of data, the consistency in the data collection techniques, a low resource setting, and a zero-hour attack. The performance of the model is affected by most of these problems. In this section we will talk about difficulties in recognizing threats to IoT protection and counter-measuring study based on AI, and present some strategies for overcoming these situations to be used during future studies.

A. REAL-TIME THREAT DETECTION

AI-based threat model is supposed to analyze large amounts of incoming data in real time, identify a threat, and initiate a rapid response to prevent cyber attacks until an attacker damages the system or removes data from the system. Real-time Big data analytics can examine an organization's event logs to detect threats and prevent attacks. There is scope for developing a platform for massive data analysis to identify a context-conscious attack without time delay.

B. FITTING PROBLEMS AND HYPER PARAMETERS TUNING

A ML model learns from data-sets collected from the environment/system, adjusts its learning parameters, and retains training examples. In ML model, overfitting occurs when the model learns the data (including noise in the data) too well and exhibits high variance as well as low bias. On the other hand, Under-fitting occurs when the ML model cannot learn trend of the data and shows low variance as well as high bias. Both overfitting or underfitting lead to poor performance on new data sets.

The learning behavior of the ML model depends on the hyper parameters chosen randomly or selectively, and even minor changes in these parameters can lead to significant changes in the performance of the model. The Optimization of these hyperparameters is challenging, and requires more analysis.

C. DATA SCARCITY

AI-based technique is data driven and thus, a large volume of actual data sets is required from the real-world environment which is the AI-based model's building block. In order to achieved anticipated performance, this high volume of data is divided into two datasets called training and testing data. Then the model is learnt with balanced and unbiased training dataset and observed the performance of the model with testing dataset. However, the generation of huge volume of clean and noiseless data samples is still a challenge.

D. CYBER THREATS

IoT nodes are resource-constrained and can not apply complex security algorithms. If ML model is used for securing IoT nodes, the model may use a portion of node-generated data. Thus a compromised node may have dire effects on vital applications such as smart grid or healthcare. Therefore, protecting the node and data input into ML and DL systems is essential. Ensuring node protection is also one of the biggest research challenges.

E. LATENCY

Real-time IoT applications (such as driverless vehicles, healthcare, banking and supply-chain, online banking, etc.) use limitless training data to create a deterministic ML model. In real-time, IoT systems are typically stochastic and random, thus the existing models are not applicable for real-time applications. RL and its DL variants suffer from delays due to the reward/penalty calculation. This needs new ML frameworks that can be trained online via dynamic streaming data and ensure low latency real-time intelligence.

F. EFFICIENCY AND IOT CAPABILITY TRADE OFF

The IoT requires a balance between security and energy consumption. The increase of IoT security increases processing (overhead security data) and power requirements of linked IoT nodes (sending / receiving security-related data). Security can also be costly, both directly in terms of software and hardware costs and indirectly in relation to energy usage. For the many industrial IoT applications which rely on the use of large numbers of connected sensors at inaccessible locations, low energy consumption and low maintenance costs are a prerequisite. For the researcher, then energy efficient protection measures are an open challenge.

VII. CONCLUSION

The IoT technology has managed to become an increasingly noticeable part of our everyday lives. The security and privacy concerns of IoT are indeed very critical to make commercial success. The IoT network security techniques and methods could be compromised due to the heterogeneity and complex existence of the IoT networks. AI and ML techniques can be utilized to ensure the countermeasure of IoT threats. These approaches have created self-organizing routines that can function very well in the system and thus increase overall system performance (e.g., human users and IoT devices). Distributed learning strategies are built in, so there is no central control board necessary. There are still no usable datasets for ML- and DL-based protection systems, so it is difficult to evaluate how efficient their functions are in practice. We have listed the security issues of the IoT, attack vectors, and security needs. We discussed various models and hypotheses for IoT security. In addition, we have noticed limited investigation is made in this field. Firstly, we reviewed security strategies and outlined open problems and future study. Since the theoretical basis of AI and ML is still lagging, specific ways to optimize the efficiency of AI and ML models are still in need of being decided. Several new learning methods and novel visualization techniques will be important for accurate and thorough data comprehension.

ACKNOWLEDGMENT

The authors would like to thank Brac University for supporting this research.

COMPLIANCE WITH ETHICAL STANDARDS

Funding: None.

Conflicts of Interest: Authors declare no conflicts of Interest.

Ethical Approval: No ethical approval required for this study.

Authors and Contributors: This work was carried out in close collaboration between all co-authors. All authors have seen and approved the final version of the manuscript.

REFERENCES

[1] H. A. Abdul-Ghani and D. Konstantas, “A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective,” Journal of Sensor and Actuator Networks, vol. 8, no. 2, p. 22, Jun. 2019, number: 2 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2224-2708/8/2/22

[2] F. K. Santoso and N. C. H. Vun, “Securing iot for smart home system,” in 2015 International Symposium on Consumer Electronics (ISCE), 2015, pp. 1–2.

[3] H. N. Rafsanjani and A. Ghahramani, “Towards utilizing internet of things (iot) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings,” Journal of Building Engineering, vol. 27, p. 100948, 2020.

[4] F. Loukil, C. Ghedira-Guegan, A. N. Benharkat, K. Boukadi, and Z. Maamar, "Privacy-Aware in the IoT Applications: A Systematic Literature Review," in On the Move to Meaningful Internet Systems. OTM 2017 Conferences, ser. Lecture Notes in Computer Science, H. Panetto, C. Debruyne, W. Gaaloul, M. Papazoglou, A. Paschke, C. A. Ardagna, and R. Meersman, Eds. Cham: Springer International Publishing, 2017, pp. 552–569.

[5] S. Aheleroff, X. Xu, Y. Lu, M. Aristizabal, J. Pablo Velásquez, B. Joa, and Y. Valencia, "IoT-enabled smart appliances under industry 4.0: A case study," Advanced Engineering Informatics, vol. 43, p. 101043, Jan. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1474034620300124

[6] P. J. Basford, F. M. J. Bulot, M. Apetroaie-Cristea, S. J. Cox, and S. J. Ossont, "LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation," Sensors, vol. 20, no. 3, p. 648, Jan. 2020, number: 3 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/20/3/648

[7] E. Symeonaki, K. Arvanitis, and D. Piromalis, "A Context-Aware Middleware Cloud Approach for Integrating Precision Farming Facilities into the IoT toward Agriculture 4.0," Applied Sciences, vol. 10, no. 3, p. 813, Jan. 2020, number: 3 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2076-3417/10/3/813

[8] M. S. Kaiser, K. T. Lwin, M. Mahmud, D. Hajializadeh, T. Chaipimonplin, A. Sarhan, and M. A. Hossain, "Advances in crowd analysis for urban applications through urban event detection," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 10, pp. 3092–3112, 2018.

[9] T. d. Vass, H. Shee, and S. J. Miah, "Iot in supply chain management: a narrative on retail sector sustainability," International Journal of Logistics Research and Applications, vol. 0, no. 0, pp. 1–20, 2020, publisher: Taylor & Francis _eprint: https://doi.org/10.1080/13675567.2020.1787970. [Online]. Available: https://doi.org/10.1080/13675567.2020.1787970

[10] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," SN Applied Sciences, vol. 2, no. 1, p. 139, Dec. 2019.

[11] M. A. Burhanuddin, A. A.-J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10, no. 1-7, pp. 17–21, Feb. 2018, number: 1-7.

[12] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1899–1909, 2017.

[13] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[14] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Future Generation Computer Systems, vol. 108, pp. 909–920, Jul. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17321003

[15] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[16] N. Su, Y. Zhang, and M. Li, "Research on data encryption standard based on aes algorithm in internet of things environment," in 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2019, pp. 2071–2075.

[17] K.-H. Han and W.-S. Bae, "Proposing and verifying a security protocol for hash function-based IoT communication system," Cluster Computing, vol. 19, no. 1, pp. 497–504, Mar. 2016. [Online]. Available: https://doi.org/10.1007/s10586-015-0518-9

[18] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," Future Generation Computer Systems, vol. 96, pp. 481–489, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18327237

[19] F. De Rango, G. Potrino, M. Tropea, and P. Fazio, "Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks," Pervasive and Mobile Computing, vol. 61, p. 101105, Jan. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119219304705

[20] J. Höglund, S. Lindemer, M. Furuhed, and S. Raza, "PKI4IoT: Towards public key infrastructure for the Internet of Things," Computers & Security, vol. 89, p. 101658, Feb. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404819302019

[21] Z. A. Al-Odat, S. K. Srinivasan, E. M. Al-Qtiemat, and S. Shuja, "A Reliable IoT-Based Embedded Health Care System for Diabetic Patients," arXiv, pp. 1–11, Aug. 2019, arXiv: 1908.06086. [Online]. Available: http://arxiv.org/abs/1908.06086

[22] H. Zhang, J. Yu, C. Tian, L. Tong, J. Lin, L. Ge, and H. Wang, "Efficient and secure outsourcing scheme for rsa decryption in internet of things," IEEE Internet of Things Journal, pp. 1–1, 2020.

[23] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Future Generation Computer Systems, vol. 78, pp. 964–975, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X1630694X

[24] D. A. F. Saraiva, V. R. Q. Leithardt, D. de Paula, A. Sales Mendes, G. V. González, and P. Crocker, "PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices," Sensors, vol. 19, no. 19, p. 4312, Jan. 2019, number: 19 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/19/19/4312

[25] F. M. Santa and H. M. Ariza, "Secure Information Transmission Device Implemented on an Embedded System using 3DES and AES Algorithms," Int. J. Eng. Res. Technol., vol. 12, no. 11, pp. 1950–1956, 2019.

[26] D. P. Bhatt, L. Raja, and S. Sharma, "Light-weighted cryptographic algorithms for energy efficient applications," Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 2, pp. 643–650, Dec. 2020.

[27] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New Lightweight DES Variants," in Fast Software Encryption, ser. Lecture Notes in Computer Science, A. Biryukov, Ed. Berlin, Heidelberg: Springer, 2007, pp. 196–210.

[28] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for iot devices," in 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018, pp. 1–8.

[29] F. Loukil, C. Ghedira-Guegan, A. N. Benharkat, K. Boukadi, and Z. Maamar, "Privacy-Aware in the IoT Applications: A Systematic Literature Review," in On the Move to Meaningful Internet Systems. OTM 2017 Conferences, ser. Lecture Notes in Computer Science, H. Panetto, C. Debruyne, W. Gaaloul, M. Papazoglou, A. Paschke, C. A. Ardagna, and R. Meersman, Eds. Cham: Springer International Publishing, 2017, pp. 552–569.

[30] S. W. Yahaya, A. Lotfi, and M. Mahmud, "A consensus novelty detection ensemble approach for anomaly detection in activities of daily living," Appl. Soft Comput., vol. 83, p. 105613, 2019.

[31] ——, "Towards a data-driven adaptive anomaly detection system for human activity," Pattern Recognition Letters, vol. 145, pp. 200–207, 2021.

[32] M. Fabietti, M. Mahmud, A. Lotfi, A. Averna, D. Guggenmo, R. Nudo, and M. Chiappalone, "Neural network-based artifact detection in local field potentials recorded from chronically implanted neural probes," in Proc. IJCNN, 2020, pp. 1–8.

[33] H. M. Ali, M. S. Kaiser, and M. Mahmud, "Application of Convolutional Neural Network in Segmenting Brain Regions from MRI Data," in Brain Informatics, ser. Lecture Notes in Computer Science, P. Liang, V. Goel, and C. Shan, Eds. Cham: Springer International Publishing, 2019, pp. 136–146.

[34] M. Mahmud, M. S. Kaiser, A. Hussain, and S. Vassanelli, "Applications of Deep Learning and Reinforcement Learning to Biological Data," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 6, pp. 2063–2079, Jun. 2018.

[35] M. Mahmud, M. S. Kaiser, T. McGinnity, and A. Hussain, "Deep Learning in Mining Biological Data," Cogn. Comput., vol. 13, no. 1, pp. 1–33, Jan. 2021.

[36] M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, and A. Hussain, "A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications," Cogn. Comput., vol. 10, no. 5, pp. 864–873, 2018.

[37] M. Mahmud and M. S. Kaiser, "Machine Learning in Fighting Pandemics: A COVID-19 Case Study," in COVID-19: Prediction, Decision-Making, and its Impacts, ser. Lecture Notes on Data Engineering and Communications Technologies, K. Santosh and A. Joshi, Eds. Singapore: Springer, 2021, pp. 77–81.

[38] M. B. T. Noor, N. Z. Zenia, M. S. Kaiser, M. Mahmud, and S. Al Mamun, "Detecting Neurodegenerative Disease from MRI: A Brief Review on a Deep Learning Perspective," in Brain Informatics, ser. Lecture Notes in

Computer Science, P. Liang, V. Goel, and C. Shan, Eds. Cham: Springer International Publishing, 2019, pp. 115–125.

[39] M. B. T. Noor, N. Z. Zenia, M. S. Kaiser, S. Al Mamun, and M. Mahmud, "Application of deep learning in detecting neurological disorders from magnetic resonance images: a survey on the detection of alzheimer's disease, parkinson's disease and schizophrenia," Brain informatics, vol. 7, no. 1, pp. 1–21, 2020.

[40] J. Ruiz, M. Mahmud, M. Modasshir, M. S. Kaiser, f. t. Alzheimer's Disease Neuroimaging Initiative et al., "3d densenet ensemble in 4-way classification of alzheimer's disease," in International Conference on Brain Informatics. Springer, 2020, pp. 85–96.

[41] Y. Miah, C. N. E. Prima, S. J. Seema, M. Mahmud, and M. S. Kaiser, "Performance comparison of machine learning techniques in identifying dementia from open access clinical datasets," in Proc. ICACIn. Springer, Singapore, 2021, pp. 79–89.

[42] N. Dey, V. Rajinikanth, S. Fong, M. Kaiser, and M. Mahmud, "Social-group-optimization assisted kapur's entropy and morphological segmentation for automated detection of covid-19 infection from computed tomography images," Cogn. Comput., vol. 12, no. 5, pp. 1011–1023, 2020.

[43] V. M. Aradhya, M. Mahmud, B. Agarwal, and M. Kaiser, "One shot cluster based approach for the detection of covid-19 from chest x-ray images," Cogn. Comput., pp. 1–9, 2021, [Online First, doi: 10.1007/s12559-020-09774-w].

[44] A. K. Singh, A. Kumar, M. Mahmud, M. S. Kaiser, and A. Kishore, "Covid-19 infection detection from chest x-ray images using hybrid social group optimization and support vector classifier," Cogn. Comput., pp. 1–13, 2021, [Online First, doi: 10.1007/s12559-021-09848-3].

[45] H. R. Bhapkar, P. N. Mahalle, G. R. Shinde, and M. Mahmud, "Rough Sets in COVID-19 to Predict Symptomatic Cases," in COVID-19: Prediction, Decision-Making, and its Impacts, ser. Lecture Notes on Data Engineering and Communications Technologies, K. Santosh and A. Joshi, Eds. Singapore: Springer, 2021, pp. 57–68.

[46] M. H. Al Banna, K. A. Taher, M. S. Kaiser, M. Mahmud, M. S. Rahman, A. S. Hosen, and G. H. Cho, "Application of artificial intelligence in predicting earthquakes: state-of-the-art and future challenges," IEEE Access, vol. 8, pp. 192 880–192 923, 2020.

[47] S. Jesmin, M. S. Kaiser, and M. Mahmud, "Artificial and internet of healthcare things based alzheimer care during covid 19," in International Conference on Brain Informatics. Springer, 2020, pp. 263–274.

[48] ——, "Towards artificial intelligence driven stress monitoring for mental wellbeing tracking during covid-19," in Proc. WI-IAT'20, 2021, pp. 1–6.

[49] M. Nahiduzzaman, M. Tasnim, N. T. Newaz, M. S. Kaiser, and M. Mahmud, "Machine learning based early fall detection for elderly people with neurological disorder using multimodal data fusion," in Proceedings of the 13th International Conference on Brain Informatics. Springer, 2020, pp. 204–214.

[50] M. J. Al Nahian, T. Ghosh, M. N. Uddin, M. M. Islam, M. Mahmud, and M. S. Kaiser, "Towards artificial intelligence driven emotion aware fall monitoring framework suitable for elderly people with neurological disorder," in Proceedings of the 13th International Conference on Brain Informatics. Springer, 2020, pp. 275–286.

[51] M. J. Al Nahian et al., "Towards an accelerometer-based elderly fall detection system using cross-disciplinary time series features," IEEE Access, pp. 1–13, 2021, [Online First].

[52] O. Orojo, J. Tepper, T. M. McGinnity, and M. Mahmud, "A Multi-recurrent Network for Crude Oil Price Prediction," in Proc. IEEE SSCI. IEEE, 2019, pp. 2953–2958.

[53] M. Kaiser et al., "iworksafe: Towards healthy workplaces during covid-19 with an intelligent phealth app for industrial settings," IEEE Access, vol. 9, pp. 13 814 – 13 828, 2021.

[54] J. Watkins, M. Fabietti, and M. Mahmud, "Sense: a student performance quantifier using sentiment analysis," in Proc. IJCNN, 2020, pp. 1–6.

[55] G. Rabby, S. Azad, M. Mahmud, K. Z. Zamli, and M. M. Rahman, "TeKET: a Tree-Based Unsupervised Keyphrase Extraction Technique," Cogn. Comput., vol. 12, no. 4, pp. 811–833, Mar. 2020.

[56] M. S. Kaiser, K. Lwin, M. Mahmud, D. Hajializadeh, T. Chaipimonplin, A. Sarhan, and M. Hossain, "Advances in crowd analysis for urban applications through urban event detection," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 10, pp. 3092–3112, 2018.

[57] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," arXiv:1901.07309 [cs], Jan. 2019, arXiv: 1901.07309. [Online]. Available: http://arxiv.org/abs/1901.07309

[58] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180–187.

[59] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," arXiv:1903.00846 [cs], Feb. 2020, arXiv: 1903.00846. [Online]. Available: http://arxiv.org/abs/1903.00846

[60] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199–221, Aug. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618301208

[61] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Communications Surveys Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

[62] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," in 2012 International Conference on Computer Science and Electronics Engineering, vol. 3, 2012, pp. 648–651.

[63] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 17–31, Sep. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870515000141

[64] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," in 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sep. 2019, pp. 1–5.

[65] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. 118–137, Apr. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864817300214

[66] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for iot devices," in 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018, pp. 1–8.

[67] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "Iot security techniques based on machine learning: How do iot devices use ai to enhance security?" IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, 2018.

[68] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, Jul. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804520301041

[69] S. Zeadally and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," International Journal of Communication Systems, vol. 33, no. 1, p. e4169, 2020, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/dac.4169. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4169

[70] S. Gupta, S. Vyas, and K. P. Sharma, "A survey on security for iot via machine learning," in 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020, pp. 1–5.

[71] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, p. 100059, Sep. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2542660519300241

[72] M. Amiri-Zarandi, R. A. Dara, and E. Fraser, "A survey of machine learning-based solutions to protect privacy in the Internet of Things," Computers & Security, vol. 96, p. 101921, Sep. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404820301978

[73] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the internet of things and wireless sensor networks via machine learning: A survey," in 2018 International Conference on Computer and Applications (ICCA), 2018, pp. 215–218.

[74] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," arXiv:1904.05735 [cs, stat], Mar. 2019, arXiv: 1904.05735. [Online]. Available: http://arxiv.org/abs/1904.05735

[75] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," arXiv:1807.11023 [cs], Jul. 2018, arXiv: 1807.11023. [Online]. Available: http://arxiv.org/abs/1807.11023

[76] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," Procedia Computer Science, vol. 171, pp. 1251–1260, Jan. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050920311121

[77] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study," arXiv:2006.15340 [cs], Jul. 2020, arXiv: 2006.15340. [Online]. Available: http://arxiv.org/abs/2006.15340

[78] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Systems, vol. 189, p. 105124, Feb. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950705119304897

[79] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019.

[80] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Computer Networks, vol. 151, pp. 147–157, Mar. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618308739

[81] N. Moustafa, J. Hu, and J. Slay, "A holistic review of Network Anomaly Detection Systems: A comprehensive survey," Journal of Network and Computer Applications, vol. 128, pp. 33–55, Feb. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804518303886

[82] L. Oliveira, J. J. P. C. Rodrigues, S. A. Kozlov, R. A. L. Rabêlo, and V. H. C. d. Albuquerque, "MAC Layer Protocols for Internet of Things: A Survey," Future Internet, vol. 11, no. 1, p. 16, Jan. 2019, number: 1 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1999-5903/11/1/16

[83] S. M. Sajjad and M. Yousaf, "Security analysis of ieee 802.15.4 mac in the context of internet of things (iot)," in 2014 Conference on Information Assurance and Cyber Security (CIACS), 2014, pp. 9–14.

[84] A. Salihbegovic, T. Eterovic, E. Kaljic, and S. Ribic, "Design of a domain specific language and ide for internet of things applications," in 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015, pp. 996–1001.

[85] B. Negash, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "LISA: Lightweight Internet of Things Service Bus Architecture," Procedia Computer Science, vol. 52, pp. 436–443, 2015, conference Name: The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015) Publisher: Elsevier. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-168960

[86] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "Rpl-based routing protocols in iot applications: A review," IEEE Sensors Journal, vol. 19, no. 15, pp. 5952–5967, 2019.

[87] A. Rayes and S. Salam, "The Internet in IoT—OSI, TCP/IP, IPv4, IPv6 and Internet Routing," in Internet of Things From Hype to Reality: The Road to Digitization, A. Rayes and S. Salam, Eds. Cham: Springer International Publishing, 2017, pp. 35–56. [Online]. Available: https://doi.org/10.1007/978-3-319-44860-2_2

[88] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications," Sensors, vol. 19, no. 9, p. 2144, Jan. 2019, number: 9 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/19/9/2144

[89] A. Rayes and S. Salam, "The Internet in IoT," in Internet of Things From Hype to Reality: The Road to Digitization, A. Rayes and S. Salam, Eds. Cham: Springer International Publishing, 2019, pp. 37–65. [Online]. Available: https://doi.org/10.1007/978-3-319-99516-8_2

[90] P. Danielis, H. Puttnies, E. Schweissguth, and D. Timmermann, "Real-time capable internet technologies for wired communication in the industrial iot-a survey," in 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, 2018, pp. 266–273.

[91] S. Seleznev and V. Yakovlev, "Industrial Application Architecture IoT and protocols AMQP, MQTT, JMS, REST, CoAP, XMPP, DDS," International Journal of Open Information Technologies, vol. 7, no. 5, pp. 17–28, Apr. 2019, number: 5. [Online]. Available: http://www.injoit.ru/index.php/j1/article/view/737

[92] J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," Int. J. Comput. Appl., vol. 90, no. 11, pp. 20–26, 2014.

[93] G. Ambika and P. Srivaramangai, "A study on data security in internet of things," Intl. J. Comput. Trends Technol., vol. 5, no. 02, pp. 464–469, 2017.

[94] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. 118–137, Apr. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864817300214

[95] N. Baracaldo, B. Chen, H. Ludwig, A. Safavi, and R. Zhang, "Detecting poisoning attacks on machine learning in iot environments," in 2018 IEEE International Congress on Internet of Things (ICIOT), 2018, pp. 57–64.

[96] M. Fredrikson, S. Jha, and T. Ristenpart, "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures," in CCS '15, 2015.

[97] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine learning-based jamming detection in wireless iot networks," in 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 2019, pp. 1–5.

[98] Y. Gwon, S. Dastangoo, C. Fossa, and H. T. Kung, "Competing mobile network game: Embracing antijamming and jamming strategies with reinforcement learning," in 2013 IEEE Conference on Communications and Network Security (CNS), 2013, pp. 28–36.

[99] M. A. Aref, S. K. Jayaweera, and S. Machuzak, "Multi-agent reinforcement learning based cognitive anti-jamming," in 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017, pp. 1–6.

[100] L. Xiao, Y. Li, G. Liu, Q. Li, and W. Zhuang, "Spoofing detection with reinforcement learning in wireless networks," in 2015 IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–5.

[101] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 10 037–10 047, 2016.

[102] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT," in Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Chennai India: ACM, Jul. 2017, pp. 1–10. [Online]. Available: https://dl.acm.org/doi/10.1145/3084041.3084061

[103] A. Hamza, H. H. Gharakheili, and V. Sivaraman, "Combining MUD Policies with SDN for IoT Intrusion Detection," in Proceedings of the 2018 Workshop on IoT Security and Privacy, ser. IoT S&amp;P '18. Budapest, Hungary: Association for Computing Machinery, Aug. 2018, pp. 1–7. [Online]. Available: https://doi.org/10.1145/3229565.3229571

[104] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–5.

[105] M. A. Khatun, N. Chowdhury, and M. N. Uddin, "Malicious nodes detection based on artificial neural network in iot environments," in 2019 22nd International Conference on Computer and Information Technology (ICCIT), 2019, pp. 1–6.

[106] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," arXiv:1709.04647 [cs], Sep. 2017, arXiv: 1709.04647. [Online]. Available: http://arxiv.org/abs/1709.04647

[107] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, "DeepRing: Protecting Deep Neural Network With Blockchain," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, 2019, pp. 1–8.

[108] "A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers - Tri-Hai Nguyen, Myungsik Yoo, 2017." [Online]. Available: https://journals.sagepub.com/doi/full/10.1177/1550147717739157

[109] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home iot devices," in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2015, pp. 163–167.

[110] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," 2018 IEEE Security and Privacy Workshops (SPW), pp. 29–35, May 2018, arXiv: 1804.04159. [Online]. Available: http://arxiv.org/abs/1804.04159

[111] P. Shukla, "Ml-ids: A machine learning approach to detect wormhole attacks in internet of things," in 2017 Intelligent Systems Conference (IntelliSys), 2017, pp. 234–240.

[112] Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi, and N. A. Malik, "Proposing a rank and wormhole attack detection framework using machine learning," in 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019, pp. 1–9.

[113] "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach - ScienceDirect." [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366416306387

[114] M. N. Napiah, M. Y. I. Bin Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (cha - ids) for 6lowpan communication protocol," IEEE Access, vol. 6, pp. 16 623–16 638, 2018.

[115] R. Singh, J. Singh, and R. Singh, "Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks," 2017, iSSN: 1530-8669 Library Catalog: www.hindawi.com Pages: e3548607 Publisher: Hindawi Volume: 2017.

[116] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao, "You are how you click: Clickstream analysis for sybil detection," in 22nd {USENIX} Security Symposium ({USENIX} Security 13), 2013, pp. 241–256.

[117] B. Farzaneh, M. Koosha, E. Boochanpour, and E. Alizadeh, "A new method for intrusion detection on rpl routing protocol using fuzzy logic," in 2020 6th International Conference on Web Research (ICWR), 2020, pp. 245–250.

[118] H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, "Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol," Apr. 2019, iSSN: 1076-2787 Library Catalog: www.hindawi.com Pages: e6516253 Publisher: Hindawi Volume: 2019. [Online]. Available: https://www.hindawi.com/journals/complexity/2019/6516253/

[119] I. Farris, J. B. Bernabe, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, and B. Sahlin, "Towards provisioning of sdn/nfv-based security enablers for integrated protection of iot systems," in 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017, pp. 169–174.

[120] K. V. V. N. L. S. Kirana et al., "Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques - ScienceDirect." [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920312497

[121] P. Ghadekar, N. Doke, S. Kaneri, and V. Jha, "Secure access control to iot devices using blockchain." [Online]. Available: https://www.google.com/search?q=secure+access+control+to+iot+devices+using+blockchain&oq=Secure+Access+Control+to+IoT+Devices+using+Blockchain&aqs=chrome.0.0j69i60.766j0j9&sourceid=chrome&ie=UTF-8

[122] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in 2018 International Joint Conference on Neural Networks (IJCNN), 2018, pp. 1–8.

[123] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "Sdn-based data transfer security for internet of things," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 257–268, 2018.

[124] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for iot devices using an sdn gateway," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 157–163.

[125] F. Li, A. Shinde, Y. Shi, J. Ye, X. Li, and W. Song, "System statistics learning-based iot security: Feasibility and suitability," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6396–6403, 2019.

[126] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home iot using openflow," in 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 147–156.

[127] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A. Sadeghi, "DÏot: A federated self-learning anomaly detection system for iot," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019, pp. 756–767.

[128] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, "Lightweight classification of iot malware based on image recognition," in 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), vol. 02, 2018, pp. 664–669.

[129] P. Feng, J. Ma, C. Sun, X. Xu, and Y. Ma, "A novel dynamic android malware detection system with ensemble learning," IEEE Access, vol. 6, pp. 30 996–31 011, 2018.

[130] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," IEEE Access, vol. 6, pp. 12 118–12 128, 2018.

[131] I. Alrashdi, A. Alqazzaz, R. Alharthi, E. Aloufi, M. A. Zohdy, and H. Ming, "Fbad: Fog-based attack detection for iot healthcare in smart cities," in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON), 2019, pp. 0515–0522.

[132] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," IEEE Communications Magazine, vol. 56, no. 2, pp. 169–175, 2018.

[133] S. O. Uwagbole, W. J. Buchanan, and L. Fan, "Numerical encoding to tame sql injection attacks," in NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 1253–1256.

[134] C. Chung, J. Cui, P. Khatkar, and D. Huang, "Non-intrusive process-based monitoring system to mitigate and prevent vm vulnerability explorations," in 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013, pp. 21–30.

[135] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation," IEEE Access, vol. 6, pp. 43 472–43 488, 2018.

[136] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Šrndić, P. Laskov, G. Giacinto, and F. Roli, "Evasion Attacks against Machine Learning at Test Time," in Machine Learning and Knowledge Discovery in Databases, ser. Lecture Notes in Computer Science, H. Blockeel, K. Kersting, S. Nijssen, and F. Železný, Eds. Berlin, Heidelberg: Springer, 2013, pp. 387–402.

[137] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in iot networks," in GLOBECOM, 2019, pp. 1–6.

[138] Y. E. Sagduyu, Y. Shi, and T. Erpek, "Iot network security from the perspective of adversarial deep learning," in 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2019, pp. 1–9.

[139] N. Papernot, P. McDaniel, and I. Goodfellow, "Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples," arXiv:1605.07277 [cs], May 2016, arXiv: 1605.07277. [Online]. Available: http://arxiv.org/abs/1605.07277

[140] J. Liu, Z. Zhao, X. Cui, Z. Wang, and Q. Liu, "A novel approach for detecting browser-based silent miner," in 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 2018, pp. 490–497.

[141] A. Kumar and T. J. Lim, "EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques," arXiv:1906.09715 [cs], Jun. 2019, arXiv: 1906.09715. [Online]. Available: http://arxiv.org/abs/1906.09715

[142] J. Mao, J. Bian, W. Tian, S. Zhu, T. Wei, A. Li, and Z. Liang, "Phishing page detection via learning classifiers from page layout feature," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, p. 43, Feb. 2019. [Online]. Available: https://doi.org/10.1186/s13638-019-1361-0

[143] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web Phishing Detection Using a Deep Learning Framework," Wireless Communications and Mobile Computing, vol. 2018, p. 4678746, Sep. 2018, publisher: Hindawi. [Online]. Available: https://doi.org/10.1155/2018/4678746

[144] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 769–773.

[145] E. Ciklabakkal, A. Donmez, M. Erdemir, E. Suren, M. K. Yilmaz, and P. Angin, "ARTEMIS: An Intrusion Detection System for MQTT Attacks in Internet of Things," 2019 38th Symposium on Reliable Distributed Systems (SRDS), 2019.

[146] A. Dehghantanha, A. Azmoodeh, and K.-K. R. Choo, "Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning," IEEE Transactions on Sustainable Computing, Feb. 2018, publisher: IEEE. [Online]. Available: https://doi.org/10.1109/TSUSC.2018.2809665

[147] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786, 2016.

[148] T. Alves, R. Das, and T. Morris, "Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers," IEEE Embedded Systems Letters, vol. 10, no. 3, pp. 99–102, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8332522/

[149] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in iot using sdn," in 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), 2017, pp. 1–6.

[150] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," IEEE Transactions on Communications, vol. 67, no. 2, pp. 1371–1387, 2019.

[151] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp. 2087–2091.

[152] L. Xiao, X. Wan, and Z. Han, "Phy-layer authentication with multiple landmarks with reduced overhead," IEEE Transactions on Wireless Communications, vol. 17, no. 3, pp. 1676–1687, 2018.

[153] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," Journal of Parallel and Distributed Computing, vol. 119, pp. 18–26, Sep. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731518302004

[154] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," The Journal of Supercomputing, vol. 74, no. 10, pp. 5156–5170, Oct. 2018. [Online]. Available: https://doi.org/10.1007/s11227-018-2413-7

[155] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in iot networks," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0452–0457.

[156] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, Jul. 2018, arXiv: 1805.03409. [Online]. Available: http://arxiv.org/abs/1805.03409

[157] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2089–2100, 2013.

[158] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep Learning for Detection of Routing Attacks in the Internet of Things," International Journal of Computational Intelligence Systems, vol. 12, no. 1, pp. 39–58, Nov. 2018, publisher: Atlantis Press. [Online]. Available: https://www.atlantis-press.com/journals/ijcis/25905181

[159] A. Verma and V. Ranga, "Elnids: Ensemble learning based network intrusion detection system for rpl based internet of things," in 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1–6.

[160] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home iot devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042–9053, 2019.

[161] M. Pourvahab and G. Ekbatanifard, "An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology," IEEE Access, vol. 7, pp. 99 573–99 588, 2019, conference Name: IEEE Access.

[162] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in iot using sdn," in 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), 2017, pp. 1–6.

[163] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, "Continuous security in iot using blockchain," in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 6423–6427.

[164] H. Naeem, B. Guo, and M. R. Naeem, "A light-weight malware static visual analysis for iot infrastructure," in 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), 2018, pp. 240–244.

[165] E. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb, "MalDozer: Automatic framework for android malware detection using deep learning," Digital Investigation, vol. 24, pp. S48–S59, Mar. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287618300392

[166] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," Applied Soft Computing, vol. 72, pp. 79–89, Nov. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1568494618303508

[167] B. Sudqi Khater, A. W. B. Abdul Wahab, M. Y. I. B. Idris, M. Abdulla Hussain, and A. Ahmed Ibrahim, "A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing," Applied Sciences, vol. 9, no. 1, p. 178, Jan. 2019, number: 1 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2076-3417/9/1/178

[168] S. Rathore, B. Wook Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," Journal of Network and Computer Applications, vol. 143, pp. 167–177, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804519302243

[169] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, "Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network," IEEE Access, vol. 6, pp. 73 713–73 723, 2018, conference Name: IEEE Access.

[170] R. Komiya, I. Paik, and M. Hisada, "Classification of malicious web code by machine learning," in 2011 3rd International Conference on Awareness Science and Technology (iCAST), 2011, pp. 406–411.

[171] H. Fang, A. Qi, and X. Wang, "Fast authentication and progressive authorization in large-scale iot: How to leverage ai for security enhancement," IEEE Network, vol. 34, no. 3, pp. 24–29, 2020.

[172] E. M. Dovom, A. Azmoodeh, A. Dehghantanha, D. E. Newton, R. M. Parizi, and H. Karimipour, "Fuzzy pattern tree for edge malware detection and categorization in IoT," Journal of Systems Architecture, vol. 97, pp. 1–7, Aug. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1383762118305265