International Journal of Research in Engineering, Science and Management
Volume 6, Issue 3, March 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Machine Learning Techniques to Combat Security Threats in Social Internet of Things

R. Sunitha[1*], J. Chandrika[2], H. C. Pavithra[3]
[1]Associate Professor, Department of Artificial Intelligence and Machine Learning, B. N. M. Institute of Technology, Bangalore, India
[2]Professor and Head, Department of Information Science and Engineering, Malnad College of Engineering, Hassan, India
[3]Assistant Professor, Department of Artificial Intelligence and Machine Learning, B. N. M. Institute of Technology, Bangalore, India

***Abstract*: A new IoT archetype in which items can create social relationships with one another based on user preferences, resulting in a social platform is known as the Social Internet of Things (SIoT). Machines and gadgets in almost any commercial enterprise may be linked and programmed to offer facts to cloud apps and return end the usage of mobile networks. The act of securing net gadgets and the networks to which they're linked from threats and breaches is referred to as protection inside the Social Internet of Things. Identifying, protecting, and tracking threats, in addition to supporting the restoration of vulnerabilities from some of the technology which could constitute protection hazards, are all methods to offer protection. The blessings of SIoT are apparent, however high-profile assaults, blended with uncertainties regarding approximately protecting good practices and their associated costs, are deterring many companies from imposing it. Here, we are surveying a few machine-learning solutions that address the problem of social internet of things security. Any enterprise trying to secure SIoT devices on a more scalable and efficient basis with automation and aberrant behavior detection can benefit from machine learning. The performance of various machine learning algorithms and tools like Decision Tree (DT), Naive Bayes (NB), K-Nearest Neighbors (KNN), and Artificial Neural Networks (ANN), etc., in discovering the vulnerabilities and threats in SIoT is discussed here.**

***Keywords*: Social Internet of Things, Machine Learning, Threats, Vulnerabilities, Artificial Neural Network.**

1. Introduction

As new technology stacks are developed, the IT cyber ecology is constantly changing. However, many of these solutions have not been thoroughly vetted in terms of security, and they are frequently targeted by cyber thieves. When faced with the extent of cyber threats and the intricacy of finely built malicious software program that continuously evolves and changes, signature-primarily based totally detection strategies end up useless. Big Data, Distributed Data Mining, and Machine Learning answers, on the opposite hand, are making progress. Now cybersecurity answers are geared up with field-proven, effective, and scalable answers, permitting device directors to look at diverse factors from diverse angles with various degrees of detail. Countering dangerous software program is certainly considered one among cutting-edge cybersecurity challenges [1]. Malware samples are commonly well-crafted pc packages that try and stay quiet at the same time as tracking compromised infrastructures and property in notable detail. Infected computers frequently join through a telecommunication network to establish a botnet, which hackers may efficiently operate from a central location for various nefarious reasons such as DDoS assaults, SPAM distribution, sensitive data thefts, and extortion attacks, and so on. Machine learning and data mining techniques have advanced in the field of Big Data, introducing new tools to aid in the fight against malware. Distributed algorithm for pattern classification and extraction is also offered by many authors.

As attacks get more sophisticated, the security issues in SIoT are increasing. According to Milosevic et al. [2], effective computing equipment, including computer PCs, can be capable of pick out malware using state-of-the-art resources. SIoT gadgets, on the opposite hand, have restrained resources. Traditional cybersecurity structures and software program, meanwhile, are useless at detecting tiny assault versions or zero-day assaults [3], due to the fact each should be up to date on a normal basis. Furthermore, the seller does now no longer offer real-time updates, leaving the community exposed. Machine Learning (ML) techniques may be used to enhance SIoT infrastructure (including wise sensors and SIoT gateways) [4] in addition to cybersecurity device performance [5]. These algorithms might also additionally experiment community traffic, replace hazard information databases, and preserve the underlying structures steady from new assaults primarily based totally on present day cyber-hazard information [6]. The researchers have all started using the groundbreaking Blockchain (BC) technique to guard the underlying structures similarly to ML algorithms [7]. Although ML algorithms and BC strategies had been created to fight cyber dangers withinside the SIoT area, integrating the 2 is a brand new frontier that should be explored.

Figure 1 depicts the many cyber security objectives in the social internet of things. Many studies are focused on achieving security goals such as authentication, authorization, integrity, non-repudiation, privacy, policy enforcement, confidentiality, trust, middleware security, and mobile security in the context of the SIoT environment, platforms, devices, and communication, among other things.

*Corresponding author: sunithar1389@gmail.com

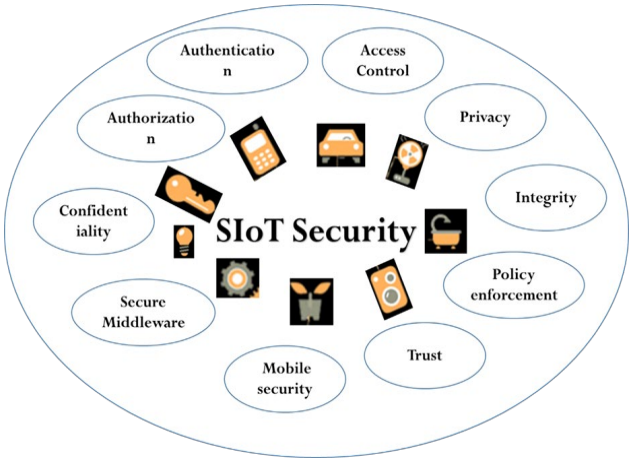

Fig. 1. Cyber security concerns in Social Internet of Things

According to Yang et al. [8], the Internet of Things is constructed as a community of small gadgets unfold throughout a huge region. An anomaly detection-primarily based totally technique become supplied to shield the safety of statistics aggregation from fake statistics injection (FDI) assaults using nation estimation and sequential speculation trying out to resolve the constraints of current studies. The important intention of the studies become to apply the vast spatial-temporal correlation among successive statistics in SIoT environmental surveillance to forecast destiny observations primarily based totally on previous observations. The authors used a game-theoretical evaluation to evaluate the proposed scheme's protection features. The findings monitor that the recommended approach has an excessive capability for detecting a compromised aggregator, even supposing the aggregator conducts an assault.

Another current ballot with the aid of using Alvarenga et al. [9] seems at safety challenges, drastically in terms of SIoT and the relationship of real-global gadgets with the Internet, on the grounds that cybersecurity risks have end up part of maximum people's day by day lives. Attacks on key infrastructures, like strength flora and public transportation, have the capacity to devastate towns and whole countries. The authors provided an observe on SIoT intrusion detection structures approaches, in addition to a taxonomy for classifying the papers applied on this observe, which became primarily based totally on standards which includes detection method, IDS deployment strategy, safety threat, and validation strategy. It became additionally stated that IDS studies for SIoT continues to be in its early tiers and that the proposed answers do now no longer cowl an extensive kind of scenarios.

Concerns concerning intrusion vulnerabilities in IoT devices were raised by Neisse et al. [10]. The work offered a Model-based Security Toolkit that is incorporated into an IoT device management framework that allows for the formulation and quick evaluation of security policies in order to secure user data. The study proposed a framework-integrated Model-based Security Toolkit that allows users to control and secure their data. The research was used to examine the feasibility and performance of a smart city scenario. The suggested paradigm allowed several sorts of trust relationships and features to be specified to control device interactions in IoT-based ecosystems.

This version takes under consideration a reference device to outline the consider elements, and it aids withinside the introduction of expressive consider-primarily based totally safety policies. Still, withinside the quest to hit upon viable intrusions or vulnerabilities in IoT, any other work, evolved with the aid of using Airehrour et al. [11], indicated a hobby in investigating IoT routing protocols and their vulnerability to assaults. To the high-quality of the author's knowledge, this became the primary observe of its kind to offer an extensive evaluation of diverse study's findings and advise answers associated with stable routing protocols amongst IoT gadgets. The Internet of Things became hooked up with the aid of using the evolution of community concept and structure in tandem with the improvement of sensors and microprocessors, and packages which includes clever houses and clever towns at the moment are turning into extensively used. Gartner estimates that 5.8 billion endpoints can be deployed in 2020, up 21% from 2019 [12]. The IoT enterprise became worth $a hundred ninety billion in 2018 and is predicted to upward thrust to $1102.6 billion with the aid of using 2026, with a compound annual boom rate (CAGR) of 24.7 percentage over that point frame [13]. The biggest marketplace percentage belongs to banking and monetary services, observed with the aid of using records generation and telecommunications.

A major share of the total IoT industry is devoted to healthcare and government applications. the IoT's fast expansion has the potential to connect billions of devices and exchange data for a variety of applications. The wonderful traits that IoT gives have additionally ended in a slew of latest safety and privateness risks, that are a huge problem for SIoT adoption's long-time period viability. Due to their restrained resources, SIoT gadgets are often mentioned to have vulnerabilities, making them an attractive goal for assault. Many and different linked gadgets released a focused assault on area call employer Dyn [14], growing a denial of service (DoS) assault in opposition to many well-known web sites like GitHub, Twitter, and others. The Mirai botnet used default usernames and passwords on the various gadgets exploited on this assault.

Despite the truth that linked independent cars (CAVs) are a wonderful sort of IoT, assaults had been provided that display how an Internet-enabled automobile is probably managed remotely thru a vulnerability withinside the media manipulate device, ensuing in critical bodily injury [15]. Many IoT apps run on embedded CPUs with restrained reminiscence and battery capability that allows you to be green and light-weight to deploy. Many IoT device designs emphasize computational performance barriers as a likely assault vector for safety and privateness concerns. IoT gadgets are usually hired as essential controllers in essential infrastructures and offer beneficial data. Stuxnet [16] is a famous malicious laptop malicious program that became designed to assault a particular commercial manipulate device (the Uranium Enrichment Plant), halting Iran's nuclear weapons program. IoT technology are essential for enhancing real-global packages together with healthcare,

clever houses, and monitoring. The vital requirement in records generation structures these days is to offer affordable safety in opposition to community threats. Perfect penetration strategies and intrusions, which includes hybrid assaults and fast-spreading clever insects and Trojans, are forcing a dynamic development of community safety answers.

Intrusion Detection/Prevention Systems (IDS-IPS) is getting used as one of the number one laptop community safety inspection strategies. Their process is to maintain a watch on and hit upon assaults on records device resources. Unauthorized get admission to to resources, efforts to dam the laptop device, and the setup of malware which includes insects or Trojan horses are the maximum not unusual place assaults. The fundamental advantage of IDS structures is that they'll be used now no longer simplest to become aware of a success assaults however additionally to reveal and report efforts to compromise the safety of the attacked records structures [8].

IDS methods are categorized into two categories. The first grouping comprises systems that employ a way of identifying known assaults through the use of predetermined, unique traits known as signatures. An another group collects the systems using a strategy based on observing the system's standard operation in order to detect anomalies that could indicated as an intrusion. This enables the detection of intrusion attempts involving many network connections. Network probing and port scanning are examples of the aforementioned attacks [9]. The capacity to distinguish unknown threats is the primary advantage of anomaly detection technology. It is not dependent on the way in which an information in attacker, but rather on what will not conform to network traffic norms. As a result, intrusion detection and prevention systems based on anomalies are more effective in detecting unknown, new attack types than systems based on signatures. The following sections will give the overview, literature, and summary of the various machine learning techniques to solve cyber issues, threats, and vulnerabilities.

2. Background

The complexity of cyber protection has swiftly extended as ICT technology development and new stacks are advised and created, rendering the conventional signature-primarily based totally method ineffective. Many of present-day current answers have by no means been very well tested in phrases of protection. Big Data technology, on the alternative hand, offer community managers with a huge variety of equipment to fight cyber threats. One such device for community site visitor's evaluation and anomaly detection is supplied on this study. The device's center is constructed on Big Data processing, information mining, and device getting to know algorithms. So far, the proposed device makes use of batch processing tactics to perform sample extraction algorithms. The experiments given right here are centered with regards to botnet identity the usage of information withinside the shape of NetFlow.

The overall performance assessment of the proposed algorithms is the situation of the evaluation of the consequences. Different settings are explored particularly in an effort to examine traits inclusive of detection efficacy. The received findings are encouraging, indicating that the proposed answer might be a precious device for community administrators [17]. Because of the tremendous use of SIoT gadgets in lots of programs, consumers' protection and privateness have turn out to be predominant concerns. Cyber risks are swiftly evolving, rendering modern protection and privateness answers ineffective. As a result, all people at the Internet is a hacker's product. As a result, Machine Learning (ML) strategies are used to extract dependable consequences from vast, complex databases, which may also then be applied to forecast and hit upon vulnerabilities in SIoT-primarily based totally systems.

In addition, Blockchain (BC) tactics are getting more and more more famous in contemporary-day SIoT programs to cope with protection and privateness concerns. ML algorithms and BC tactics have each been the situation of numerous investigations. However, those research use ML algorithms or BC tactics to cope with both protection or privateness troubles, necessitating a mixed evaluation of modern efforts to cope with each protection and privateness troubles the usage of ML algorithms and BC strategies.

The authors present a review of research activities in the SIoT area over the last few years, from 2008 to 2019, tackling security and privacy challenges using ML algorithms and BC approaches. First, the authors have gone over and identified the numerous security and privacy concerns that have been documented in the SIoT sector over the last twelve years. Finally, the authors used ML algorithms and BC techniques to address security and privacy issues in the IoT domain [18], and they have highlighted and illuminated various challenges and future research possibilities.

3. Social Internet of Things Architecture and threats

A traditional SIoT system is typically epitomized in five basic layers: a) perception, b) service, c) application, and d) network. Figure 2 depicts many tiers of these systems, as well as the threats and vulnerabilities that reveal the anticipated flaws in SIoT security. [7] examines a variety of security concerns with the hopes of developing innovative, more realistic, and resilient solutions. Figure 2 depicts the basic levels of general SIoT engineering. Each layer's security challenges are explored separately, with new robust and feasible arrangements sought.

A. Social Internet of Things architecture

1) Belief layer

The belief layer of a SIoT version is worried with the sensors in SIoT gadgets for statistics collection, and processing is carried out thru technology which includes RFID, WSN, RSN, and GPS. The bodily layer has diverse sensors for looking at measurements which includes temperature, humidity, pressure, altitude, and different parameters, in addition to role identity functions [8]. The assets to be had to the nodes are limited, and they may be additionally required to have a distributive shape of their organization, in addition to the bodily layer protection threats indexed underneath and additionally diverse cyber protection threats and vulnerabilities with inside the Social

Internet of things, are depicted in parent 2.

1) *Physical Attacks on SIoT Devices:* These are hardware-associated assaults on SIoT gadgets that necessitate near bodily proximity among the attacker and the SIoT machine with a view to be successful. The following are a few examples of regarded attacks of this type: a. Tampering: The assault is done both via way of means of bodily harming the nodes, both via way of means of changing the whole node or a part of the hardware, or via way of means of the use of digital interrogation to get get right of entry to to and alternate touchy statistics which includes keys and routing statistics. b. Malicious Code: The nodes right here had been infiltrated via way of means of malicious software program that has been bodily implanted with a view to scouse borrow get right of entry to a SIoT machine.
2) *Impersonation:* In a dispensed machine, authentication is difficult, consequently antagonistic nodes create a phony identification with a view to dedicate collusions.
3) *Denial-of-service (DoS) Attacks:* In this case, the attackers compromise the nodes' processing capability, rendering them unavailable.
4) *Routing Attacks:* Compromised nodes withinside the center of the statistics accumulating and transmission manner alter the precise routing path. These eventualities have an effect on WSN extra than others.
5) *Data Transmission Attacks:* These compromise the confidentiality of statistics and the integrity of the statistics transmission mechanism. Sniffing and MITM are examples of this sort of assault.

2) Network layer

This layer guarantees that the simple stage is obtainable from anywhere. This stage's most important reason is to transmit the received statistics from the primary stage to every other machine for processing throughout any community this is used by all get right of entry to networks (4G, WiFi, MANET) or the internet. [9] offers a large evaluate of the safety troubles that stand up in a mobile wi-fi community. According to this study, while in comparison to preceding generations of mobile networks, the numerous and open frameworks of an LTE community, which might be generally IP-based, are extra inclined in phrases of protection. At this time, the subsequent are the maximum urgent protection issues which can stand up:

1) Routing Attacks: Malicious code withinside the center can alternate routing choices and tables, in addition to create harm at some stage in the statistics seize and transmission procedure.
2) Denial-of-service (DoS) Attacks: Because SIoT is engaged and heterogeneous, the shipping layers are extra prone to assaults.
3) Data Transit Attacks: These assaults can compromise the confidentiality and integrity of touchy statistics whilst it's miles being transmitted thru to be had networks or thru get right of entry to permits.

3) Service layer

The protection in SIoT layout is the purpose for including a fourth layer. In a three-layer architecture, statistics is routed immediately to the community layer. The threat of receiving assaults will increase while statistics is dispatched immediately to the community layer. A new layer is proposed due to issues with inside the three-layer machine. Information from a belief layer is brought to a help layer in a four-layer architecture. The help layer is accountable for things. It guarantees that statistics is dispatched via way of means of valid customers and that it's miles secure from dangers. There are several strategies for verifying customers and statistics. Authentication is the maximum extensively used mechanism. Pre-shared secrets, keys, and passwords are used to enforce it. The help layer's 2d obligation is to ship statistics to the community layer. Wireless and stressed out media may be used to ship statistics from the help layer to the community layer. This layer is prone to a whole lot of attacks, inclusive of DoS assaults, malicious insider assaults, unlawful get right of entry to, and so on. The following are a number of the help layer's maximum not unusual place dangers and troubles:

1) *DoS Attack:* In a help layer, a DoS assault is tied to the community layer. To flood community traffic, an attacker sends a great quantity of statistics. As a end result of the huge utilization of machine assets, the SIoT is exhausted, and the person is not able to get right of entry to the machine.
2) *Malicious Insider Attack:* This sort of assault takes place from inside a SIoT surroundings to advantage get right of entry to to customers' private statistics. It is done via way of means of a certified person with a view to advantage get right of entry to the statistics of every other person. It's a completely unique and complicated assault that necessitates a whole lot of protection strategies [19,20].

4) Application layer

These are the layers that in shape the wishes of the clients. When purchasers question this layer, it may provide information including atmospheric pressure, temperature, and different such measurements. This layer is vital for SIoT improvement because it serves as a basis for showing the numerous wishes of clients if you want to create multi-motive SIoT gadgets. This layer may be used to construct and put into effect numerous SIoT ecosystems. For a higher recognition of clever computing, the programs are subjected to help its sub-stage in all offerings provided.

1) *Data Leakage:* Having know-how of the safety troubles withinside the application makes information robbery distinctly easy (for each attackers and customers).
2) *DoS-primarily based totally assaults:* These assaults have the capacity to damage carrier nodes or the whole software.
3) *Harmful Codes:* Knowing approximately present vulnerabilities permits a few malicious code to be injected into the application.

The protection issue of SIoT gadgets is both left out or seemed as a postproduction step through manufacturers. This technique stems mainly from the preference to attain a speedy time to marketplace and low-value manufacturing at the same time as leaving protection dangers unaddressed. There are only some devices that offer rudimentary safety the use of software

program-primarily based totally strategies. As an end result of the emphasis on software program-primarily based totally safety, the hardware is prone to attacks that had been now no longer planned. It is apparent from work [20] that if the hardware isn't always steady, it's going to continuously cause the software program being susceptible as well. This phase delves into the advent of techniques for assuring protection in IoT gadgets, in addition to the variations among it and conventional records era protection.

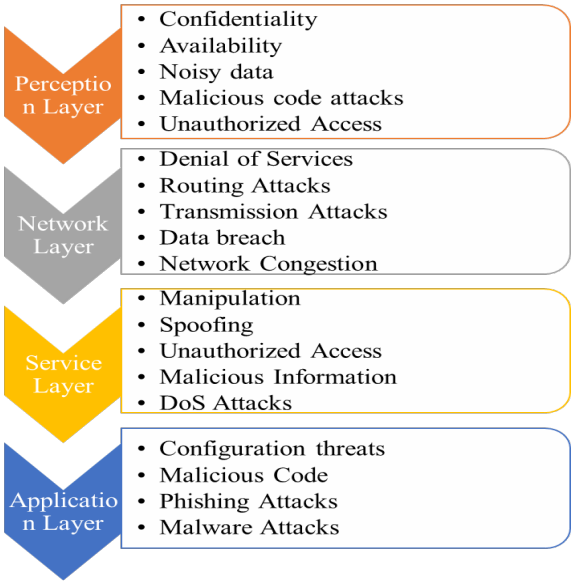

Fig. 2. Cyber protection threats and vulnerabilities in Social Internet of matters

B. *Security Threats in SIoT*

The Social Internet of Things (SIoT) refers to a massive variety of heterogeneous social sensing gadgets that speak with each other in a network throughout a LAN or the Internet. Because of the to be had sources of stop gadgets, SIoT threats fluctuate from conventional community assaults [22]. The Social Internet of Things has restricted reminiscence and computing capability, while the conventional Internet has effective servers and computer systems with lots of sources. As an end result, multifactor protection stages and complex protocols may be used to steady a conventional community, that's something that an actual-time SIoT machine cannot do. SIoT gadgets, in contrast to conventional networks, use much less steady wi-fi conversation protocols including LoRa, ZigBee, 802.15.4, and 802.11a/b/n/g/p. Finally, IoT gadgets have various information contents and codecs because of software-unique capability and the dearth of a not unusual place working machine, making it tough to construct a uniform protection protocol [23]. Because of those flaws, SIoT is prone to plenty of protection and privateness dangers, developing possibilities for several kinds of assaults.

The CIA trinity of Confidentiality of the information, Integrity of the information, and Availability of the community [24, 25, 26] is on the coronary heart of protection and privateness. A user's figuring out records, packets introduced from a surveillance digital digicam to a vacation spot server, a command issued to a vehicle thru a key-fob, or a multimedia dialogue among people are all examples of information with inside the Internet of Things. Any illegal information disclosure should jeopardize the confidentiality, integrity, or availability of the records. It is a privateness danger whilst a danger compromises confidentiality. Data integrity and community availability are each compromised through protection dangers. Few threats in SIoT are mentioned right here at the side of the few present answers designed through numerous authors.

1) *Denial of Service*

In evaluation to all different protection threats, Denial of Service (DoS) has the maximum trustworthy implementation. In addition, because the variety of SIoT gadgets with insufficient protection capabilities grows, DoS has grown to be a famous tactic for attackers. The principal intention of a DoS assault is to flood the community with bogus requests, inflicting community sources to be depleted, including bandwidth. As an end result, actual customers are not able to get right of entry to the offerings. DDoS (Distributed Denial of Service) is an extra superior shape of DoS attack wherein numerous re-assets assault an unmarried goal, making it extra tough to pick out and avoid [27, 26, 29, 30, 31, 32]. DDoS attacks are available plenty of forms, however they usually have the identical intention. SYN flooding [33] (wherein an attacker sends a chain of SYN requests to a goal), Internet Control Message Protocol (ICMP) assaults [34] (wherein a massive variety of ICMP packets are broadcasted the use of the victim's spoofed IP), crossfire assaults [35] (wherein an attacker makes use of a complicated and hugely massive-scale botnet for assault execution), and User Datagram Protocol (UDP) flooding assaults [36] are a few examples of (sending a massive variety of UDP packets to random ports on a faraway victim).

In an IoT community, a botnet attack [96] is a kind of DDoS assault. A botnet is a set of Internet of Things nodes (gadgets) which have been hacked if you want to release an assault on a unique goal, including a financial institution server. As defined in [37], botnet assaults may be executed the use of plenty of protocols, along with Message Queuing Telemetry Transport (MQTT), Domain Name Server (DNS), and Hypertext Transfer Protocol (HTTP). Several answers are given for stopping DoS with inside the IoT environment. Diro et al. [38] used Deep Learning (DL) methodologies' self-gaining knowledge of abilities to stumble on an attack in a fog-to-matters environment. Abeshu et al. [27] advocated controlling the DDoS assault through the use of allotted DL on fog computing in every other study. Tan et al [39] Proposed an Intrusion Detection System (IDS) is a fixed of studies efforts to save you DDoS assaults making use of modern ML and DL algorithms [30, 31]. Flooding issues in Software Defined Networks had been highlighted through Sharma et al. and Tselois et al. [29, 32], respectively (SDN). The loss of authentication withinside the plain-textual content TCP channel made the SDN's pinnacle layer prone to brute pressure assaults, in step with the study.

2) Man-in-the-middle

Man-in-the-middle (MiTM) assaults are one of the earliest cyber-assaults [40]. MiTM assaults consist of such things as spoofing and impersonation. For example, a node X trying to engage with vacation spot B can also additionally rather be speaking with a MiTM attacker posing as vacation spot B. In SSL striping, an attacker can use such strategies to connect with the server with an HTTPS connection at the same time as speaking with the goal on an unsecured HTTP connection. Recently, many research has centered on enhancing the safety in opposition to MiTM assaults [41, 42, 43, 44]. Ahmad et al. [41] mentioned a healthcare state of affairs wherein an affected person is robotically given an insulin dosage. This sort of application is prone to a MiTM assault, which may be fatal. For example, Tang et al. [45] determined vulnerabilities with inside the community carrier libraries of cell apps, which would possibly disclose the apps' visitors to MiTM assaults.

Chatterjee et al., [46], in reaction to impersonation assaults, highlighted present strategies of authentication in wi-fi cell gadgets that applied a mystery key. This key turned into saved in non-risky reminiscence and turned into used for virtual signatures and hash-primarily based totally encryption. This technique turned into now no longer best susceptible, however it turned into additionally inefficient in phrases of power. Similarly, cross-site-recovery-forgery (CSRF) assaults have an effect on OAuth 2.0, the maximum latest and broadly used IoT standard. The OAuth protocol calls for guide tool authentication, that's time-ingesting. Wang et al. [44] noted a physical-layer protection difficulty in Wi-Fi authentication in every other research. They claimed that the prevailing speculation take a look at for detecting an Eve in Wi-Fi networks, which compares radio channel records with Alice's channel record, is regularly unavailable, mainly in dynamic networks.

3) Malware

The term "malware" refers to malevolent software program. The variety of SIoT gadgets has been growing in latest years, as has the frequency of SIoT software program patches, which may be utilized by an attacker to put in malware on a tool and do dangerous operations. Viruses, spyware, worms, trojan horses, rootkits, and malvertising are all examples of malware [47, 48]. Smart domestic gadgets, scientific equipment, and car sensors are only a few examples of what may be hacked. Malware at the Internet of Battlefield Things turned into investigated through Azmoodeh et al. [50]. (IoBT). These types of attackers are regularly state-sponsored, well-funded, and well-trained. Using exceptional supervised ML algorithms, Aonzo et al. [49], Feng et al. [51], and Wei et al. [52] sought to guard useful resource-restrained android gadgets from malware assaults. [53, 54, 55] presented an in depth research of malware detection and highlighted numerous protection flaws withinside the Android platform, mainly at the software layer, which incorporates programs with plenty of components.

C. Machine Learning Techniques to offer SIoT Protection

Machine learning could be an effective tool for any corporation looking to automate and detect abnormal behavior in SIoT devices in a more scalable and efficient manner. A machine learning (ML) approach to SIoT security can help with some of these difficulties. It solves the challenge of recognizing new devices on a network, ensuring that they are incorporated into the existing security framework, and making SIoT maintenance easier for busy IT staff. SIoT devices are often the weakest link in a company's network, yet they are extremely valuable. It's simple to see why corporations continue to use them when you consider their scalability. Cybersecurity teams require more technology to keep track of all the devices and keep the network safe.

By automating the scanning and control of SIoT devices throughout the whole network, ML can secure SIoT in general. They can monitor the entire network for risks and shut them down before IT personnel are even aware of them. In 2018, Microsoft's Windows Defender program did just that, stopping a Trojan malware attack in under 30 minutes. Further, machine learning can assist in detecting all devices on a network, including those that only connect on a periodic basis. It can automate network segmentation plan deployment by automatically allocating devices to the appropriate segment based on pre-defined rules. IT staff may now focus on more important technology projects and better manage the company's entire cybersecurity strategy.

Access manipulate for IoT structures in heterogeneous networks with severa varieties of nodes and multi-supply information is tough to design [85]. For intrusion detection, device gaining knowledge of techniques including SVM, K-NN, and neural networks had been applied [86]. For example, proposes the use of multivariate correlation evaluation to extract geometrical correlations among community visitor’s capabilities if you want to stumble on DoS assaults. When as compared to the triangular area-primarily based totally nearest neighbor's approach with KDD Cup 99 information set, this scheme improves detection accuracy through 3.05 percentage to 95.2 percentage.

Anomaly intrusion detection answers in SIoT structures generally have reduced detection overall performance because of useful resource and compute constraints in SIoT gadgets including sensors outdoors. Machine gaining knowledge of techniques help with inside the improvement of light-weight get right of entry to manipulate mechanisms that keep strength and increase the lifestyles of IoT structures. For example, the outlier identity method proposed in [86] makes use of K-NN to clear up the trouble of unsupervised outlier detection in WSNs and affords flexibility in defining outliers at the same time as ingesting much less strength. When as compared to a Centralized scheme with identical common strength use, this scheme can also additionally keep the maximum strength through 61.4 percentage.

In Microsoft's Windows Defender example, client-aspect and cloud-primarily based totally device gaining knowledge of structures examine present day community use in opposition to 30 protection prevention fashions in tandem. To decide whether or not an assault is tremendous or negative, a number of those fashions compare hundreds of thousands of factors. To guard in opposition to undiscovered vulnerabilities and zero-day

assaults, device gaining knowledge of fashions screen SIoT gadgets and community interest in actual-time, detecting uncommon conduct and taking brief shielding measures. Many device gaining knowledge of algorithms replace themselves on a normal foundation to hold up with the evolving danger landscape, making them best for defensive complicated networks. It unexpectedly examines a SIoT fleet's widespread virtual footprint and compares its conduct to regarded dangers and former conduct.

Only a community the use of device gaining knowledge of technology can stumble on threats consequently quickly earlier than they infiltrate the primary company community thru SIoT gadgets. The pace with which ML searches, detects, and protects gadgets and networks is its key gain in SIoT protection. All networks, along with the ones nevertheless using older era and SIoT gadgets, can gain from present day protection principles and frameworks. Let's take a better examine on ML benefits. Machine learning strategies including unsupervised learning, supervised learning, and reinforcement learning (RL) [56, 57] had been broadly used to enhance community protection as given in figure 3, including authentication, access control, anti-jamming offloading, and malware detection.

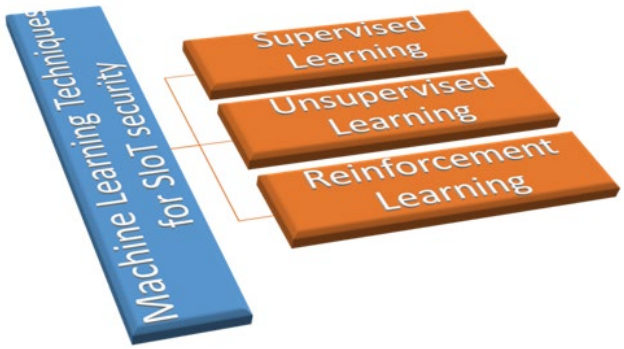

Fig. 3. Machine Learning techniques for SIoT security

1) Supervised learning techniques

The task of learning a function from input to output is called supervised machine learning. Labeled data, also called training data, contains input and output labels needed to train the machine so it can analyze the data and provide conclusions for future examples. Classification and regression machine learning are two types of supervised machine learning. The temporal classification model is used about 80% of the time. If the output variable is a category, such as B. Identifying gender (male or female) or blood type (A+, B+, O, B), machine learning is used for classification.

Pattern recognition is what classification machine learning is all about. If the output is an actual value, such as B. weight, percentage or other, machine regression learning is used. The following are some widely used supervised learning algorithms such as Support Vector Machines (SVM), Naive Bayes, KNearest Neighbor (KNN), Neural Networks, Deep Neural Networks (DNN), and Random Forests that can be used to categorize network or application traffic. Traces of IoT devices to develop classification or regression models [58]. SVM can be used to detect network intrusions [58] and phishing attacks [59], KNN can be used to detect network intrusions [60] and malware [61], and neural networks can be used to detect network intrusions [62] and DoS attacks [63]. IoT devices can use Naive Bayes for intruder detection [58] and a random forest classifier for malware detection [61]. DNN can be used by IoT devices with sufficient computing and storage capacity to identify phishing attacks [56].

ANN [64] is another supervised method that can be used for both classification and regression. The efficiency of this algorithm is determined by the value of K. The Nave-Bayes algorithm is based on Bayes' theorem, which states that the presence of a feature in a class is independent of the presence of other features in that class. It can be used to solve binary class and multiclass problems. A decision tree is a simple graph with an attribute name at each node and a single edge that represents a flow toward a specific answer. A random forest is a collection of many decision trees, which is more accurate than using a single decision tree. K. Gurulakshmi and A. Nesarani [65] proposed a machine learning-based support vector machine that analyzes IoT malware received from a large number of IoT devices in a fixed time interval, detects the packet, and the time required for this arrive reduced. your intended goal. Even with a minimal number of datasets, SVM delivers good results.

This algorithm examines how one can learn to automatically generate correct predictions based on parameters. These functions are used to group instances in a given collection of records. The number and definition of relevant attributes as well as the number of training sets to learn affect the recognition performance in machine learning. Because of their hierarchical nature, they are resistant to outliers, scalable, and able to model nonlinear decision boundaries naturally. Authors [65] surveyed various well-known machine learning classifiers using the Bot-IoT dataset. When selecting these classifiers, the emphasis is on combining popular algorithms with various properties. The few algorithms employed in this context are briefly reviewed in the following sections.

a) *SVM:* For Internet visitors [67] and clever grid [59], SVM is used to locate numerous assaults. For example, a light-weight assault detection approach mentioned in [67] detects visitors flooding assaults the use of an SVM-primarily based totally hierarchical structure. The dataset collector machine used SNMP question messages to reap SNMP MIB statistics from the sufferer machine withinside the assault experiment. Experiments display that this approach can locate assaults at a price of over 99.50 percentage and classify them with an accuracy of over 99.53 percentage [67].

b) *K-Nearest Neighbours (KNN):* KNN is one of the maximum simple and powerful supervised getting to know algorithms to be had. It is used to look the to be had dataset for brand spanking new statistics factors which are similar to modern statistics factors [70]. KNN, which plays nicely on multidimensional statistics and is a short set of rules at some stage in the schooling phase, is gradual at some stage in the estimation stage.

c) *Quadratic Discriminant Analysis (QDA):* For supervised category applications, QDA is an extraordinary set of rules. Discriminant evaluation is a statistical technique for categorizing measured statistics into one in every of numerous corporations. When there isn't always loads of statistics in a category, QDA is a superb option. The range of samples found should be more than the range of corporations so as to use Quadratic Discriminant Analysis.

d) *Iterative Dichotomiser 3 (ID3):* ID3 is a set of rules for producing a selection tree from a fixed of statistics. Ross Quinlan [66] become the only who got here up with the idea. A selection tree is a category set of rules that employs a tree-like selection structure. It's one technique to displaying a set of rules made up totally of conditional manage statements. The traits function tree nodes, and the standards are designed to move from one node to the next, with the "leaves" representing the record's elegance values [63]. ID3 is a forerunner to the C4.5 algorithms and is normally utilized in gadget getting to know and herbal language processing.

e) *Random Forest (RF):* RF is a selection tree-primarily based totally gadget getting to know approach. A "forest" is constructed the use of this approach with the aid of using setting collectively a massive range of various selection tree systems which are shaped in diverse ways [67]. When as compared to unmarried classifiers, this approach has severa advantages, such as the capacity to run on big datasets efficiently, its small weight relative to different methods, and robustness towards noise and outliers.

f) *Adaptive Boosting (AdaBoost):* AdaBoost is a gadget getting to know approach that makes a speciality of category troubles and tries to transform inefficient classifiers into powerful ones. Freund and Schapire proposed it in 1996, and it could be used alongside numerous distinct getting to know algorithms to growth performance. The capacity of the AdaBoost set of rules to address lacking values in a dataset is its maximum important feature.

g) MLP stands for multilayer perceptron and is a form of feedforward synthetic neural community (ANN). Artificial neural networks (ANNs) are a form of gadget getting to know this is primarily based totally on how the human mind learns and derives new information. There are 3 degrees in an MLP: input, output, and hidden. For schooling, MLP employs back-propagation, a supervised getting to know technique. The neural community with neurons withinside the hidden layer is used to educate the MLP connection weights and compute the suspicion aspect that shows whether or not an IoT tool is the sufferer of DoS assaults, as given in [63]. Backpropagation (BP) is an evolutionary computation approach that makes use of debris with adjustable velocities to replace the MLP's connection weights. Particle swarm optimization (PSO) is an evolutionary computation approach that makes use of debris with adjustable velocities to replace the MLP's connection weights. If the MLP output reaches a threshold, the IoT tool beneathneath take a look at turns off the MAC and PHY layers to store electricity and amplify the community life.

h) *NB (Naive Bayes):* The NB is a famous supervised approach this is acknowledged for its truthful principles. The Naive Bayes technique is primarily based totally on Thomas Bayes' research [68]. For example, NB might be used to categorise site visitors as ordinary or atypical so as to locate intrusions. The NB classifier handles the site visitors' category capabilities separately, no matter the reality that they will be reliant on one another. NB is user-best due to a number of factors, alongside its simplicity, low sample required, and ease of implementation [66]. NB, on the alternative hand, interacts with abilties independently and is therefore now no longer capable of extract useful facts from feature verbal exchange and interactions.

2) Unsupervised Learning Techniques

Unsupervised studying strategies are the second one class of device studying and wherein fashions aren't supervised with the aid of using the usage of the schooling records. Unlike supervised device studying, no want to oversee or teach the model; instead, permit it paintings on its own. It includes operating with unlabeled records to labeled records factors the usage of capabilities or styles that resource categorization. The cause of reinforcement device studying is to praise you for doing the proper thing. Because there may be no supervised studying records, they may be compelled to research from their beyond experiences.

a) K-method Clustering

Unsupervised studying explores the similarity among unlabeled records to cluster them into diverse groups [71], while supervised studying calls for categorised records. The intention of K-method clustering is to resolve problems with the k-method clustering approach on inputs encrypted with awesome unbiased public keys. This technique is primarily based totally on non-colluding cloud servers, without an interplay among the cloud servers and the records proprietors for the duration of the process. In the semi-sincere scenario, the authors have validated that the approach is semantically secure. Furthermore, the authors show its effectiveness with the aid of using supplying experimental outcomes and evaluating them to beyond research [71]

b) Hierarchal clustering

For Dynamic and Heterogeneous Internet of Things, a Hierarchical Clustering technique [72] is used. On a real-world IoT platform, the proposed clustering technique is tested. Experiments on an IoT-based simulator are used to test aspects such as network coverage, communication costs, and power usage. To begin, the authors outlined the hierarchical clustering system model. The model is divided into two levels. With ID-

enabled devices, the lower level, also known as Layer 2, is implemented. This layer contains sensors, RFID devices, people, and other devices. Because of the tremendous energy harvesting, authors believe these gadgets will be unable to have IP. As a result, they won't be able to connect to the cloud directly. However, because of the requirements of the applications, they constitute an important aspect of the network.

c) Principle Component Analysis

Principal Component Analysis (PCA) [73] methods are appealing because they reduce complexity. PCA-based anomaly detection approaches have gotten a lot of attention in the past. However, there are still challenges with PCA, such as the choosing of principle components for reducing complexity. This paper explores PCA approaches utilized in earlier typical research works and provides a new generic distance calculation formula as well as a new PCA-based detection method for IoT networks. Several experiments are used to investigate formula parameters in this research. This method is suited for detecting network traffic anomalies quickly and with less complexity, according to the results. Anomaly detection in network traffic is one of network operators' most difficult responsibilities. Methods based on Principal Component Analysis (PCA) garnered a lot of attention among the various proposed methodologies due to their lower complexity. As a result, it's appropriate for IoT networks with restricted network resources and performance. PCA-based approaches, on the other hand, still have challenges with the selection of Principal Components (PCs) and calculation complexity.

d) Apriori set of rules

The Apriori rule sets uses a method called Iterative Method [74]. In which first, the candidate 1-item-set and the corresponding guide are searched to gain the common item-set-1 with the aid of using pruning out the item-set-1 with decrease guide. Then the closing common item-set-1 is hooked up to get the candidate common item-set-2. Meanwhile, the actual common item-set-2 is received with the aid of using filtering out the candidate common item-set-2 with decrease guide. Using this iterative approach to perform till the common k + 1 item-set can't be found, the corresponding common item-set-k is the output of the set of rules [75]. For example, the statistics set D on this examine has 4 records, namely, (1) cyber-attack, statistics protection, and cybercrime; (2) statistics breach, statistics protection, and synthetic intelligence; (three) cyber-attack, statistics breach, statistics protection, and synthetic intelligence; and (4) statistics breach and synthetic intelligence.

3) Reinforcement Learning Techniques

Reinforcement gaining knowledge of is a system gaining knowledge of mechanism, wherein the version learns with the aid of using looking at the environment. It is a feedback-primarily based totally system gaining knowledge of method, that's found out with the aid of using appearing and with the aid of using looking at the actions. There are numerous algorithms that exist in reinforcement gaining knowledge of to mention some Q-gaining knowledge of, Dyna-Q, post-choice country (PDS) [76], and deep Q-community (DQN) [77] permit an IoT tool to decide the safety protocols and essential parameters in opposition to numerous threats via trial-and-error [78]. Q-gaining knowledge of has been used to growth the overall performance of authentication [78], anti-jamming offloading [10], [19], [20], and malware detections [80], [81]. Dyna-Q for authentication and malware detection [80], PDS for malware detection [80], and DQN for anti-jamming transmission [82] are all alternatives for IoT gadgets.

a) *Q-gaining knowledge:* As a version-loose RL method, Q-gaining knowledge of is easy to assemble and has low computational complexity. For example, IoT gadgets can select their offloading statistics quotes in opposition to jamming and spoofing assaults the use of the Q-gaining knowledge of-primarily based totally offloading provided in [10]. The Q-characteristic represents the know-how received from the previous anti-jamming offloading and is the projected discounted long-time period advantage for every action-country pair. In every time slot, the Q-values are modified the use of the iterative Bellman equation primarily based totally at the cutting-edge offloading coverage, community condition, and jamming software acquired with the aid of using the IoT tool.

Table 1
Various Machine Learning techniques to achieve different security goals against attacks by using certain performance parameters

Security goal	Attacks	Machine learning techniques	Performance parameters
Secure IoT offloading	Jamming	Q-learning [90], [91] DQN [92]	Energy Consumption, SINR
Authentication	Spoofing	SVM [94] DNN [95] Q-learning [93] Dyna-Q [93] Incremental aggregated gradient [96] Distributed Frank-Wolfe [96]	AER, DA, CA, FAR, MDR
Secure IoT offloading Access control	DoS	Neural network [87] Q-learning [89] Multivariate correlation analysis [88]	DA, RME
Malware detection, Access control	Malware	Random forest [99] K-nearest neighbors [99] Q/Dyna-Q/PDS [102]	CA, TPR, FPR, DA, DL
Access control	Intrusion	Support vector machine [97] Neural network [100] Naive Bayes [97] K-NN [98]	CA, FAR, DA, RME
Authentication	Eavesdropping	Q-learning [101] Nonparametric Bayesian [103]	PPR, SDR

b) The IoT tool makes use of the -grasping set of rules to pick the offloading coverage that maximizes its cutting-edge Q-characteristic with a excessive chance at the same time as ignoring the opposite regulations with a low chance, ensuing in a tradeoff among exploration and exploitation. When in comparison to a benchmark approach furnished in [83], this scheme lowers the spoofing price with the aid of using 50% and lowers the jamming price with the aid of using 8%. An IoT tool can use Q-gaining knowledge of to select the radio channel to attain the cloud or facet tool, consistent with the Q-gaining knowledge of-primarily based totally anti-jamming transmission proposed in [84].

c) *DQN:* The DQN-primarily based totally anti-jamming transmission defined in [82] quickens the gaining knowledge of time for IoT gadgets having sufficient compute and reminiscence capability to pick the radio frequency channel. In the offloading in opposition to jamming assaults, this method improves the SINR of acquired indicators with the aid of using 8. Three% and saves 66.7 percentage of the gaining knowledge of time while in comparison to the Q-gaining knowledge of scheme [82].

d) *Dyna-Q:* The Dyna-Q malware detection method defined in [104] takes gain of the Dyna structure to examine from hypothetical reviews and select the first-class offloading strategy. This method improves gaining knowledge of overall performance with the aid of using combining actual-international protection reviews with digital reviews furnished with the aid of using the Dyna structure. For example, while in comparison to detection the use of Q-gaining knowledge of [104], this method reduces detection latency with the aid of using 30% and boosts accuracy with the aid of using 18%.

Table 1 shows the different machine learning techniques and various attacks with respect to the cyber security in the social internet of things. Along with this how-to achieve certain security goals using machine learning techniques and different performance parameters.

4. Conclusion

The Social Internet of Things (SIoT) is an Internet of Things (IoT) concept in which things can build social relationships with one another depending on user preferences, creating a social platform. Diverse internet of things devices communicates with one another and form a link in order to form a relationship. Similar traits, qualities, device types, and other factors are used to build the association. Using cell networks, machines, and matters in nearly any enterprise can be linked and configured to supply records to cloud apps and again ends. In the Social Internet of Things, protection refers back to the act of shielding net gadgets and the networks to which they're linked in opposition to assaults and breaches. Identifying, guarding, and tracking threats, in addition to supporting with inside the restore of vulnerabilities from quite a few technologies that may pose protection risks, are all examples of the way protection may be provided. At each factor of the SIoT journey, there may be a virtual protection risk, and a horde of hackers is ready to take advantage of a system's fault. At every point of the SIoT journey, there is a digital security risk, and a horde of hackers is waiting to exploit a system's fault.

Although the blessings of SIoT are clear, high-profile assaults, in addition to uncertainty concerning protection excellent practices and their related costs, are discouraging many companies from embracing it. Here, we're going to test some gadget gaining knowledge of answers for social net of factors protection. Machine gaining knowledge of can assist any business enterprise that desires to shield SIoT gadgets on a greater scalable and powerful foundation with automation and bizarre conduct detection. The effectiveness of numerous gadget gaining knowledge of strategies consisting of Decision Tree (DT), K-Nearest Neighbors (KNN), Naive Bayes (NB), and Artificial Neural Network (ANN), amongst others, in detecting SIoT vulnerabilities and threats is tested on this paper.

References

[1] Choras Michal, Kozik R., Renk R., Holubowicz W., A Practical Framework and Guidelines to Enhance Cyber Security and Privacy, in: Herrero A., Baruque B., Sedano J., Quintan H., Corchado E. (Eds), International Joint Conference CISIS'15 and ICEUTE'15, Advances in Intelligent Systems and Computing, 485-496, ISBN 978-3-319-19712-8, Springer 2015.

[2] Jelena Milosevic, Miroslaw Malek, and Alberto Ferrante. 2016. A Friend or a Foe? Detecting Malware using Memory and CPU Features. In Proceedings ofthe 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016), Vol. 4. 73–84.

[3] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys Tutorials 21, 3 (third quarter 2019), 2671–2701.

[4] Guido Dartmann, Houbing Song, and Anke Schmeink. 2019. Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things. Elsevier. 1–360 pages.

[5] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. 2018. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Processing Magazine 35, 5 (2018), 41–49.

[6] Hidayet Aksu, A. Selcuk Uluagac, and Elizabeth Bentley. 2018. Identification of Wearable Devices with Bluetooth. IEEE Transactions on Sustainable Computing (2018), 1–1.

[7] Kai Fan, Shangyang Wang, Yanhui Ren, Kan Yang, and Zheng Yan. 2018. Blockchain-based Secure Time Protection Scheme in IoT. IEEE Internet of Things Journal PP, c (2018),

[8] L. Yang, C. Ding, M. Wu, K. Wang, Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance, Comput. Networks 129 (2017) 410–428. Special Issue on 5G Wireless Networks for IoT and Body Sensors.

[9] B.B. Zarpelao, R.S. Miani, C.T. Kawakani, S.C. Alvarenga, A survey of intrusion detection in internet of things, J. Netw. Comput. Appl. 84 (2017) 25–37.

[10] R. Neisse, G. Steri, I.N. Fovino, G. Baldini, Seckit: a model-based security toolkit for the internet of things, Comput. Secur. 54 (Supplement C) (2015) 60–76.

[11] D. Airehrour, J. Gutierrez, S.K. Ray, Secure routing for internet of things: a survey, J. Netw. Comput. Appl. 66 (2016) 198–213.

[12] G. Egham, "5.8 billion enterprise and automotive IoT: endpoints will be in use in 2020," 2020, https://www.gartner.com/en/newsroom/pressreleases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotiveio

[13] F.ortune Business Insights, "COVID-19 impact: high dependency on novel technology to bode well for market," 2020, https://www.fortunebusinessinsights.com/industry-reports/inter netof-things-iot-market-100307

[14] Wikipedia, “2016 dyn cyberattack,” 2020. https://en.wikipedia.org/w/index.php?title=2016%20Dyn%20cyberattack&oldid=763071700

[15] A. Greenberg, “Hackers remotely kill a jeep on the highway—with me in it,” 2020, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[16] R. Langner, “Stuxnet: dissecting a cyberwarfare weapon,” IEEE Security & Privacy Magazine, vol. 9, no. 3, pp. 49–51, 2011.

[17] R. Kozik, "Distributed System for Botnet Traffic Analysis and Anomaly Detection," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 330-335, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.55.

[18] Nazar Waheed, Xiangjian He, Muhammad Ikram, Muhammad Usman, Saad Sajid Hashmi, Muhammad Usman, “Security and Privacy in IoT Using Machine Learning and Blockchain: Threats & Countermeasures”, ACM CSUR Journal, 2020.

[19] Sanzgiri A., Dasgupta D. Classification of insider threat detection techniques; Proceedings of the 11th Annual Cyber and Information Security Research Conference; Oak Ridge, TN, USA. 5–7 April 2016; New York, NY, USA: ACM; 2016. p. 25.

[20] Nurse J.R., Erola A., Agrafiotis I., Goldsmith M., Creese S. Smart insiders: Exploring the threat from insiders using the Internet-of-things; Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT); Vienna, Austria. 21–25 September 2015; pp. 5–14.

[21] Fatima Hussain, Syed Ali Hassan, Rasheed Hussain, and Ekram Hossain. 2020. Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges. IEEE Communications Surveys & Tutorials c (2020), 1–1.

[22] Qi Jing, Athanasios Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. 2014. Security of the Internet of Things: Perspectives and challenges. Wireless Networks 20 (11 2014), 2481–2501.

[23] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni. 2019. Anatomy of Threats to the Internet of Things. IEEE Communications Surveys Tutorials 21, 2 (Secondquarter 2019), 1636–1675.

[24] Magda Brewczyńska, Suzanne Dunn, and Avihai Elijahu. 2019. Data privacy laws response to ransomware attacks: A multi-jurisdictional analysis. Springer, 281–305.

[25] Pavithra Prabhu and K. N. Manjunath. 2019. Secured Image Transmission in Medical Imaging Applications—A Survey. In Computer Aided Intervention and Diagnostics in Clinical and Medical Images. Springer International Publishing, Cham, 125–133

[26] Kevin Kam Fung Yuen. 2019. Towards a Cybersecurity Investment Assessment method using Primitive Cognitive Network Process. In 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). 068–071.

[27] Abebe Abeshu and Naveen Chilamkurti. 2018. Deep Learning: The Frontier for Distributed Attack Detection in Fog-To-Things Computing. IEEE Communications Magazine 56, 2 (2018), 169–175.

[28] Abebe Diro and Naveen Chilamkurti. 2018. Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications. IEEE Communications Magazine 56, 9 (2018), 124–130.

[29] Pradip Kumar Sharma, Saurabh Singh, Young Sik Jeong, and Jong Hyuk Park. 2017. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. IEEE Communications Magazine 55, 9 (2017), 78–85.

[30] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu. 2014. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. IEEE Transactions on Parallel and Distributed Systems 25, 2 (Feb 2014), 447–456.

[31] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu. 2015. Detection of Denial-of-Service Attacks Based on Computer Vision Techniques. IEEE Trans. Comput. 64, 9 (Sep. 2015), 2519–2533.

[32] C. Tselios, I. Politis, and S. Kotsopoulos. 2017. Enhancing SDN security for iot-related deployments through blockchain. 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2017 2017-Janua (2017), 303–308.

[33] Xuyang Jing, Zheng Yan, Xueqin Jiang, and Witold Pedrycz. 2019. Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch. Information Fusion 51 (2019), 100–113.

[34] Omar E. Elejla, Bahari Belaton, Mohammed Anbar, Basim Alabsi, and Ahmed K. Al-Ani. 2019. Comparison of classification algorithms on ICMPv6-based DDoS attacks detection. Lecture Notes in Electrical Engineering 481 (2019), 347–357.

[35] Mostafa Rezazad, Matthias R. Brust, Mohammad Akbari, Pascal Bouvry, and Ngai-Man Cheung. 2018. Detecting Target-Area Link-Flooding DDoS Attacks Using Traffic Analysis and Supervised Learning. Advances in Information and Communication Networks (Dec 2018).

[36] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits. 2013. Denial-of-Service detection in 6LoWPAN based Internet of Things. In 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). 600–607.

[37] N. Moustafa, B. Turnbull, and K. R. Choo. 2019. An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. IEEE Internet of Things Journal 6, 3 (June 2019), 4815–4830.

[38] Abebe Diro and Naveen Chilamkurti. 2018. Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications. IEEE Communications Magazine 56, 9 (2018), 124–130.

[39] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A system for denial-of-service attack detection based on multivariate correlation analysis,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, pp. 447–456, Feb 2014

[40] Dan Swinhoe. 2019. What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. (2019). https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html

[41] Usman Ahmad, Hong Song, Awais Bilal, Shahzad Saleem, and Asad Ullah. 2018. Securing Insulin Pump System Using Deep Learning and Gesture Recognition. Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 (2018), 1716–1719.

[42] Muhamad Erza Aminanto, Rakyong Choi, Harry Chandra Tanuwidjaja, Paul D. Yoo, and Kwangjo Kim. 2017. Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. IEEE Transactions on Information Forensics and Security 13, 3 (2017), 621–636.

[43] Baibhab Chatterjee, Debayan Das, and Shreyas Sen. 2018. RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018 PP, c (2018), 205–208.

[44] Ning Wang, Ting Jiang, Shichao Lv, and Liang Xiao. 2017. Physical-Layer Authentication Based on Extreme Learning Machine. IEEE Communications Letters 21, 7 (2017), 1557–1560.

[45] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang, and X. Wang, “Cooperative jamming for physical layer security enhancement in internet of things,” IEEE Internet of Things Journal, vol. 5, pp. 219–228, Feb 2018.

[46] X. He, H. Dai, and P. Ning, “Improving learning and adaptation in security games by exploiting information asymmetry,” in IEEE Conf. Computer Commun. (INFOCOM), pp. 1787–1795, Hongkong, China, May 2015.

[47] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni. 2019. Anatomy of Threats to the Internet of Things. IEEE Communications Surveys Tutorials 21, 2 (Second quarter 2019), 1636–1675.

[48] Benjamin Zi Hao Zhao, Muhammad Ikram, Hassan Jameel Asghar, Mohamed Ali Kaafar, Abdelberi Chaabane, and Kanchana Thilakarathna. 2019. A Decade of Mal-Activity Reporting: A Retrospective Analysis of Internet Malicious Activity Blacklists. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. 193–205

[49] Simone Aonzo, Alessio Merlo, Mauro Migliardi, Luca Oneto, and Francesco Palmieri. 2017. Low-Resource Footprint, Data-Driven Malware Detection on Android. IEEE Transactions on Sustainable Computing 3782, c (2017), 1–1.

[50] Amin Azmoodeh, Ali Dehghantanha, and Kim-Kwang Raymond Choo. 2018. Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning. IEEE Transactions on Sustainable Computing 3782, c (2018), 1–1.

[51] P. Feng, J. Ma, C. Sun, X. Xu, and Y. Ma. 2018. A Novel Dynamic Android Malware Detection System with Ensemble Learning. IEEE Access 6 (2018), 30996–31011.

[52] Linfeng Wei, Weiqi Luo, Jian Weng, Yanjun Zhong, Xiaoqian Zhang, and Zheng Yan. 2017. Machine learning-based malicious application detection of android. IEEE Access 5 (2017), 25591–25601.

[53] Jingjing Gu, Binglin Sun, Xiaojiang Du, and Senior Member. 2018. Consortium Blockchain-Based Malware Detection in Mobile Devices. IEEE Access 6 (2018).

[54] Boohyung Lee and Jong Hyouk Lee. 2017. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. Journal of Supercomputing 73, 3 (2017), 1152–1167.
[55] Shaila Sharmeen, Shamsul Huda, Jemal H. Abawajy, Walaa Nagy Ismail, and Mohammad Mehedi Hassan. 2018. Malware Threats and Detection for Industrial Mobile-IoT Networks. IEEE Access 6 (2018), 15941–15957.
[56] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
[57] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.
[58] M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Commun. Surveys and Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.
[59] 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 Trans. Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786, Mar. 2015.
[60] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowledge and Information Systems, vol. 34, no. 1, pp. 23–54, Jan. 2013.
[61] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.
[62] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys and Tutorials, vol. 18, no. 2, pp. 1153–1176, Oct. 2015.
[63] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in Proc. Int'l Joint Conf. Neural Networks, pp. 3437–3444, Atlanta, GA, Jun. 2009
[64] J. Huang, Y. Wei, J. Yi, and M. Liu, "An improved knn based on class contribution and feature weighting," Proc. - 10th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2018, vol. 2018-Janua, pp. 313– 316, 2018.
[65] K. Gurulakshmi and A. Nesarani, "Analysis of IoT Bots Against DDOS Attack Using Machine Learning Algorithm," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 1052-1057.
[66] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," IEEE Trans. Wireless Commun., in press.
[67] J. Yu, H. Lee, M. S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Commun., vol. 31, no. 17, pp. 4212–4219, Oct. 2008.
[68] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, no. 3, pp. 680–698, Jan. 2018
[69] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in Proc. ACM Int Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 1–10, Chennai, India, Jul. 2017.
[70] X. He, H. Dai, and P. Ning, "Improving learning and adaptation in security games by exploiting information asymmetry," in IEEE Conf. Computer Commun. (INFOCOM), pp. 1787–1795, Hongkong, China, May 2015.
[71] (PDF) Secure Multi-User k-Means Clustering Based on Encrypted IoT Data from: https://www.researchgate.net/publication/344963867_Secure_Multi-User_k-Means_Clustering_Based_on_Encrypted_IoT_Data [accessed Feb 21 2022]
[72] Hierarchical Clustering for Dynamic and Heterogeneous Internet of Things. Available from: https://www.researchgate.net/publication/306073892_Hierarchical_Clustering_for_Dynamic_and_Heterogeneous_Internet_of_Things [accessed Feb 26 2022].
[73] A PCA-based method for IoT network traffic anomaly detection. Available from: https://www.researchgate.net/publication/324464302_A_PCA-based_method_for_IoT_network_traffic_anomaly_detection [accessed Feb 21 2022].
[74] Shashi, R., Dharavath, R., and Krishan, K. S. (2020). A spark-based apriori algorithm with reduced shuffle overhead. J. Supercomput. 77, 133–151.
[75] Surender, R., and Hegde, R. M. (2020). Optimal relay node selection in time-varying IoT cybers using apriori contact pattern information. Ad Hoc Netw. 98, 102–118.
[76] X. He, H. Dai, and P. Ning, "Improving learning and adaptation in security games by exploiting information asymmetry," in IEEE Conf. Computer Commun. (INFOCOM), pp. 1787–1795, Hongkong, China, May 2015.
[77] V. Mnih, K. Kavukcuoglu, D. Silver, et al., "Human-level control through deep reinforcement learning," Nature, vol. 518, no. 7540, pp. 529–533, Jan. 2015
[78] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
[79] L. Xiao, C. Xie, T. Chen, and H. Dai, "A mobile offloading game against smart attacks," IEEE Access, vol. 4, pp. 2281–2291, May 2016.
[80] L. Xiao, Y. Li, X. Huang, and X. J. Du, "Cloud-based malware detection game for mobile devices with offloading," IEEE Trans. Mobile Computing, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.
[81] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," IEEE Trans. Control of Network Systems, vol. 4, no. 3, pp. 632 – 642, Apr. 2016.
[82] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in IEEE Int'l Conf. Acoustics, Speech and Signal Processing, pp. 2087–2091, New Orleans, LA, Mar. 2017
[83] L. Xiao, C. Xie, T. Chen, and H. Dai, "A mobile offloading game against smart attacks," IEEE Access, vol. 4, pp. 2281–2291, May 2016.
[84] Y. Gwon, S. Dastangoo, C. Fossa, and H. Kung, "Competing mobile network game: Embracing anti-jamming and jamming strategies with reinforcement learning," in Proc. IEEE Conf. Commun. and Network Security (CNS), pp. 28–36, National Harbor, MD, Oct. 2013.
[85] M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Commun. Surveys and Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.
[86] J. Huang, Y. Wei, J. Yi, and M. Liu, "An improved knn based on class contribution and feature weighting," Proc. - 10th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2018, vol. 2018-Janua, pp. 313– 316, 2018.
[87] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in Proc. Int'l Joint Conf. Neural Networks, pp. 3437–3444, Atlanta, GA, Jun. 2009.
[88] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for Denial-of-Service attack detection based on multivariate correlation analysis," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 447–456, May 2013.
[89] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," IEEE Trans. Control of Network Systems, vol. 4, no. 3, pp. 632 – 642, Apr. 2016.
[90] Y. Gwon, S. Dastangoo, C. Fossa, and H. Kung, "Competing mobile network game: Embracing anti-jamming and jamming strategies with reinforcement learning," in Proc. IEEE Conf. Commun. and Network Security (CNS), pp. 28–36, National Harbor, MD, Oct. 2013.
[91] M. A. Aref, S. K. Jayaweera, and S. Machuzak, "Multi-agent reinforcement learning based cognitive anti-jamming," in Proc. IEEE Wireless Commun. and Networking Conf (WCNC), pp. 1–6, San Francisco, CA, Mar. 2017.
[92] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in IEEE Int'l Conf. Acoustics, Speech and Signal Processing, pp. 2087–2091, New Orleans, LA, Mar. 2017.
[93] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning inwireless networks," IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
[94] 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 Trans. Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786, Mar. 2015.
[95] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in Proc. ACM

Int Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 1–10, Chennai, India, Jul. 2017.

[96] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," IEEE Trans. Wireless Commun., in press.

[97] M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Commun. Surveys and Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014

[98] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowledge and Information Systems, vol. 34, no. 1, pp. 23–54, Jan. 2013.

[99] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.

[100] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys and Tutorials, vol. 18, no. 2, pp. 1153–1176, Oct. 2015.

[101] L. Xiao, C. Xie, T. Chen, and H. Dai, "A mobile offloading game against smart attacks," IEEE Access, vol. 4, pp. 2281–2291, May 2016.

[102] L. Xiao, Y. Li, X. Huang, and X. J. Du, "Cloud-based malware detection game for mobile devices with offloading," IEEE Trans. Mobile Computing, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

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

[104] L. Xiao, Y. Li, X. Huang, and X. J. Du, "Cloud-based malware detection game for mobile devices with offloading," IEEE Trans. Mobile Computing, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.