Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8669348, 12 pages
https://doi.org/10.1155/2022/8669348

Review Article

The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks

Muhammad Shafiq,[1] **Zhaoquan Gu**,[1] **Omar Cheikhrouhou**,[2] **Wajdi Alhakami**,[3] **and Habib Hamam**[4]

[1] *Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China*
[2] *CSE Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3038, Tunisia*
[3] *Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia*
[4] *Faculty of Engineering, Moncton University, NB, Canada E1A3E9*

Correspondence should be addressed to Zhaoquan Gu; zqgu@gzhu.edu.cn

Received 22 June 2022; Revised 7 July 2022; Accepted 22 July 2022; Published 3 August 2022

Academic Editor: Kuruva Lakshmanna

This paper provides an extensive and complete survey on the process of detecting and preventing various types of IoT-based security attacks. It is designed for software developers, researchers, and practitioners in the Internet of Things field who aim to understand the process of detecting and preventing these attacks. For each entry identified from the list, a brief description is provided along with references where more information can be found. However, We surveyed the current state-of-the-art IoT security solutions and focused on four main aspects: (1) handpicking representative attacks, (2) identifying potential solutions, (3) performing a threat analysis for each attack and solution, and (4) ranking solutions according to the threats they overcome. By adopting this framework, we identified five main categories of defense mechanisms: distributed denial of service detection/prevention, default password protection, encryption mechanisms, intrusion detection/prevention, and anomaly detection. These solutions are relatively mature in terms of utility and usability. However, the security analysis is conducted only concerning specific attacks, which may or may not be relevant to real-world deployment. Appropriate IoT security solutions should incorporate threat modeling while considering other factors such as resource consumption and implementation effort. Overall, evaluation of IoT security solutions is arduous due to the complexity of IoT OSes, heterogeneous IoT devices (e.g., various hardware platforms), limited availability of open-source codebases, and restrictive policies towards intellectual property disclosure. In addition, we note that there remains a lack of studies that perform a systematic evaluation of the state-of-the-art in terms of both frameworks/methodologies and mechanisms proposed.

1. Introduction

The Internet of Things (IoT) is a network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, enabling these objects to connect and exchange data. An IoT-based cyberattack is a cyberattack wherein an adversary utilizes an IoT device as part of their overall malicious action. For instance, when used in conjunction with computers or mobile phones that have been compromised by malware. As more devices are being connected to IoT every day, so are more opportunities for potential attacks. This paper surveys recent developments in detection mechanisms as well as prevention mechanisms for IoT-based security attacks. It then surveys existing cybersecurity testing standards that focus on assessing IoT-related vulnerabilities together with an overview of tools relevant to such testing efforts. Finally, it concludes with some suggestions for future research directions.

IoT is not just increasing but evolving too. Researchers have recently started working on analyzing and classifying IoT-based security attacks [1]. They identified three main categories denial of service (DoS), data manipulation, and data disclosure. Different threats exist within each category. In order to perform a successful attack on an IoT device, a number of conditions must be met. First, it must be possible to discover devices that can be attacked. Second, there should be vulnerabilities in those devices that could lead to them being compromised. Thirdly, they should connect via unsecured communication channels or protocols; otherwise, no malware could communicate with them nor send commands or exfiltrate data from them. This leads us to discuss prevention mechanisms for IoT-based security attacks in turn and then examine existing standards for testing such devices and tools relevant to such efforts [1, 2]. We also survey recent research developments related to the detection of IoT-based security attacks at several levels, including identification, monitoring, and response techniques. We conclude by summarizing our findings and making some suggestions for future research directions. IoT cyberattack classification attackers target IoT systems either to cause damage or disruption, obtain unauthorized access, or steal information. The first step toward understanding IoT cyberattacks is to classify them into types and subtypes. This can help in identifying areas where new solutions are needed for protection against these kinds of cyberattacks. Recently, we studied [3] security challenges and countermeasures for the Internet of Things [4, 5]. We classified IoT-based cyberattacks into 3 categories: (1) denial of service (DoS) [6, 7], (2) data manipulation [8], and (3) data disclosure. DoS has been widely discussed for a long time ago because it involves attacking machines through flooding network traffic without any useful purpose, usually resulting in a crash. In general, DoS attacks aim to make services unavailable in order to harm legitimate users. In contrast, data manipulation attacks aim at changing information stored in IoT devices so that attacker's goal is achieved. Data disclosure type of attack reveals sensitive user or business data without authorization. It allows attackers to get hold of personal information about individuals, their habits, and preferences. Finally, here comes a brief introduction to IoT-based security attacks in general terms before moving on to more detailed discussions about specific topics in later sections. Recently, researchers have made significant progress in developing automated methods for detecting anomalies in sensor networks using machine learning algorithms [9]. However, little work has been done so far on applying anomaly detection approaches specifically for cybersecurity applications involving connected sensors. For example, in [10], a model based on a Bayesian classifier is proposed for anomaly detection in smart grid networks. Likewise, authors in [11], a security assessment method for smart grid networks is presented. Similarly, researchers have started working on the analysis and classification of IoT-based security attacks [12]. They identified three main categories—denial of service (DoS), data manipulation, and data disclosure—different threats exist within each category. In order to perform a successful attack on an IoT device, a number of conditions must be met. First, it must be possible to discover devices that can be attacked. Second, there should be vulnerabilities in those devices that could lead to them being compromised. Thirdly, they should connect via unsecured communication channels or protocols; otherwise, no malware could communicate with them nor send commands or exfiltrate data from them. In addition to attacks aimed at devices themselves, it is equally important to consider that IoT devices may be used in attacks targeting other devices or entities. For instance, in [10], an attack model for wireless medical implantable devices is proposed. In [11], a methodology for assessing the security of M2M/IoT communications is presented. Similarly, recently, researchers have started working on the analysis and classification of IoT-based security attacks [13]. They identified three main categories denial of service (DoS), data manipulation, and data disclosure. Different threats exist within each category.

Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and network connectivity that enable these objects to collect and exchange data. The Internet of Things is a system whereby physical devices can be monitored and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems and resulting in efficiency improvements for end-users.

Security concerns are often cited as one of the main reasons why companies are not deploying IoT solutions. Many organizations do not have a clear understanding of how to address security issues when deploying an IoT solution.

The Internet of Things (IoT) is an emerging technology that uses sensors, microcontrollers, and other digital components to connect devices over the Internet. It is a broad term that covers everything from smart home products to connected vehicles.

The IoT is a great example of how technology is reshaping our lives. But it also comes with risks. There are more than 30 billion Internet-connected devices in use today, and some of them have been hacked into by malicious actors. In 2016 alone, there were approximately 1 billion data breaches worldwide, according to the Privacy Rights Clearinghouse (PRC).

In many cases, hackers have used their access to these devices to steal personal information for identity theft or financial gain. In other cases, they have caused physical damage by tampering with industrial machinery or transportation systems like trains, planes, and automobiles. The industrial control systems controlling power grids are particularly vulnerable because they are often not protected by firewalls or antivirus software, and they are difficult to update due to their complex architecture and lack of connectivity to the Internet; this makes them easy prey for hackers seeking access to critical infrastructure like hospitals.

The contribution to this survey paper is as follows:

(1) The rise of "Internet of Things": review and open research issues related to detection and prevention of IoT-based security attacks

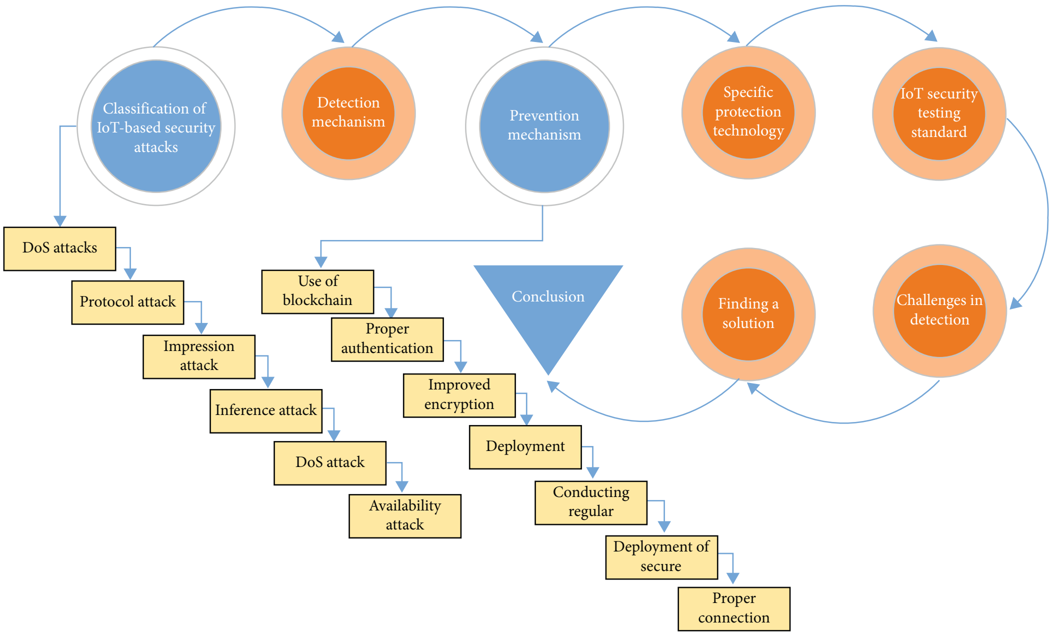

Figure 1: Proposed survey.

(2) Survey on prior work on security attacks against IoT systems

(3) Survey on protection mechanisms against security attacks against IoT systems

(4) Future research directions for detecting and preventing security attacks against IoT systems

In this paper, we review the state-of-the-art and open research issues related to the detection and prevention of IoT-based security attacks. The rise of the "Internet of Things" (IoT) is driving a new wave of cyber security attacks on IoT devices. The number of connected devices is increasing exponentially, and this trend will continue for the foreseeable future. With so many connected devices, it becomes possible for an attacker to launch an attack from any location at any time. To detect such attacks and prevent them from causing damage, we need to develop new tools and techniques to detect these attacks as soon as possible.

In this paper, we review the state-of-the-art and open research issues related to the detection and prevention of IoT-based security attacks. Recently, the number of security attacks on IoT devices has increased dramatically since there are many vulnerabilities in these devices. Many studies have been conducted focusing on detecting such attacks using machine learning techniques [3]. The main purpose of this survey is to provide a comprehensive overview of recent advances in this area by surveying relevant literature in order to identify current trends/gaps in this field so as to guide future research directions.

In Section 2, the classification of IoT-based security attacks is discussed. In Section 3, the detection mechanism for IoT-based security attacks is presented. In Section 4, an overview of existing detection and prevention mechanisms for IoT-based security attacks is given. In Section 5, specific protection technologies for specific IoT devices and services are reviewed, and in Section 6, we describe some of the important tools that can be used to test for vulnerabilities in IoT devices. In Sections 7, 8, and 9, challenges, conclusions, and recommendations for future research direction are provided. However, the flowchart of the survey is shown in Figure 1.

2. Classification of IoT-Based Security Attacks

In this paper, we tried to classify the variety of cyber threats in the Internet of Things (IoT) based on the characteristics of the threat vector, target, and attack method. A cyberattack is any violation with malicious intent carried out via a computer. This includes denial of service attacks and identity capture examples. IoT devices are "smart" physical objects which have embedded software and hardware, are connected to other devices or networks, and implement some computing-like functionality. However, the two most common categories of IoT security attacks are spoofing attacks (in which an attacker impersonates a trusted device) and denial of service (DoS) attacks. Spoofing attacks can be directed at different parts of a network, ranging from intermediary gateways to end devices. When it comes to IoT, such intermediaries are often smart hubs that connect remote devices to local networks. In many cases, these gateways do not perform authentication before establishing communication with end devices. As a result, if an attacker manages to impersonate one or more trusted device(s), they may gain access to other IoT endpoints connected to that intermediary device. This attack is commonly referred to as a man in the middle (MITM). Similarly, an attacker might try to impersonate a trusted IoT endpoint by compromising

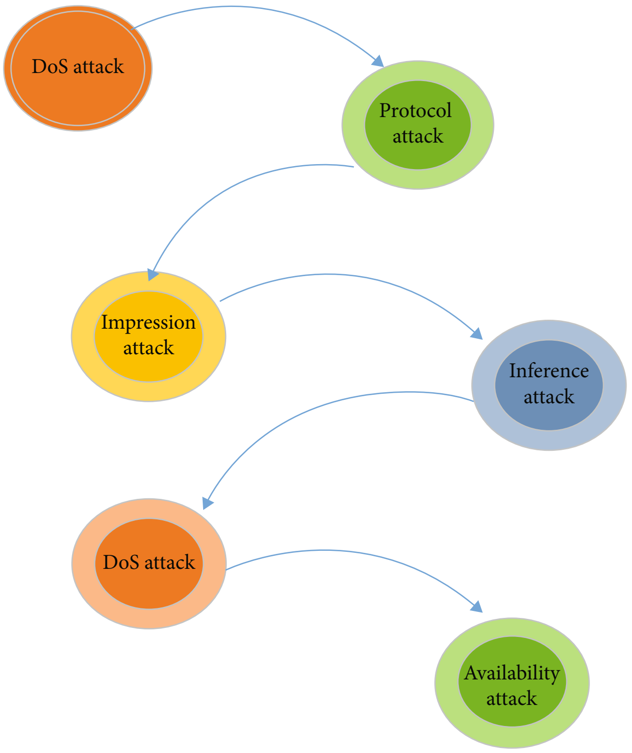

Figure 2: Classification of IoT-based security attacks.

its hardware or software. Such attacks can be particularly devastating because they allow attackers to bypass all existing IoT security measures and get direct access to IoT data. Furthermore, since IoT endpoints are usually low-power devices with limited processing power, they cannot easily detect MITM attacks. Therefore, when building IoT systems, developers should consider carefully how their products will handle MITMs. Another type of spoofing attack involves using rogue access points for eavesdropping purposes. These rogue APs are typically deployed in public places where there is no need for any sort of authentication between users and apps. However, some attacks are discussed below, and the flow chart is in Figure 2.

2.1. DoS Attack. Internet of Things is a technology that connects devices wirelessly to one another or to a control system via IoT. Every device can communicate with other devices if there is any query from their side. Thus, we can manipulate communications between different IoT devices. This can make them crash because too many connections are coming for some device at once or sending requests endlessly by using its unsecured programming code. An attacker sends so many requests that a particular device cannot handle it; hence, it is impossible for devices to protect against DoS attacks in real time. Therefore, security researchers need to come up with a solution for preventing such attacks. They must also find out how to monitor and detect these kinds of attacks. The researchers used various tools like Wireshark [14], an open-source network protocol analyzer software tool, to capture traffic packets sent over a network connection by monitoring packets traveling over a computer network or within a local area network (LAN). It allows users to see what data is being sent across networks and helps us analyze traffic patterns. Packet sniffers are used as well, but they do not allow us to decrypt encrypted data packets captured from networks. Wireshark has two main features: live capture, which allows users to capture data being transmitted across LANs or other computer networks, and file access, enabling users to save captured data into files for later analysis. With the help of Wireshark, researchers were able to observe protocols being executed by different devices connected through the Internet. Then, they could try to identify flaws and vulnerabilities in those protocols which might be exploited by attackers. Similarly, researchers also used the IDA Pro Disassembler Software program that comes under the Hex-Rays family of products. Researchers disassembled executable codes present inside each IoT device separately and then compared them with each other to find common vulnerabilities among all types of devices.

2.2. Protocol Attack. Protocol attacks are one of many ways that hackers can attempt to steal data from your network or system. They involve a hacker interacting with your network or device using protocol commands. Each type of command has a specific set of instructions that tell it what to do, how long to run, where to send information (and sometimes what information is sent), etc. And while different protocols may use different sets of instructions, they all follow a fairly similar framework about structure. Hackers take advantage of known vulnerabilities in these protocols' frameworks by attempting to redirect them from their normal operating paths—which allows them access to either restricted areas or potentially sensitive data like passwords, user names, and credit card numbers. For instance, suppose you are running a Wi-Fi router at home. In that case, there is an outside chance someone could gain access to your wireless network by intercepting unencrypted traffic between your computer and router. This kind of attack is called sniffing because it involves collecting information out in the open without being detected. What is the easiest way to prevent sniffing? Encrypt all traffic over public networks. But there are plenty more examples of protocol attacks; you just have to know where to look for them! For example, consider ARP cache poisoning.

One of our biggest concerns when talking about protocol attacks is something called man-in-the-middle (MitM) attacks. In these cases, an attacker inserts themselves into communication sessions between two people or devices—so instead of sending data directly to each other, they will instead go through whatever malicious the third party is getting involved. An easy way to think about MitM attacks would be eavesdropping; just imagine someone listening in on your phone calls rather than calling you themselves and pretending they are who they say they are, so you will give away personal details! The most common form of MitM attack involves ARP cache poisoning. This type of attack occurs when a hacker hijacks traffic by exploiting weaknesses in ARP protocols to make it appear as if their computer is actually yours—which means all information being sent from your computer will now be received by them instead. For instance, let us say you are at home trying to access a website using Wi-Fi that is connected to a router at work. But hackers have used ARP cache poisoning techniques to redirect traffic from your device over to theirs. Suppose you send out a request for that website using Wi-Fi. In that case, it will get redirected to their computer, where they can see everything you have tried accessing, including sensitive information like passwords or credit card numbers! What makes matters worse?

2.3. Impersonation Attack. An impersonation attack is a type of cyberattack wherein a malicious actor adopts or mimics another user's identity to gain unauthorized access to protected network resources. Often, an attacker will try to impersonate a high-level executive in order to bypass security controls or compromise company data. In other cases, attackers have made use of well-known public figures (such as celebrities) in efforts to trick victims into downloading malware disguised as harmless files such as picture attachments. It is important for every individual connected to an enterprise network (particularly those with elevated privileges) be aware that they may be targeted by cybercriminals engaged in impersonation attacks. The first step in preventing these types of breaches is identifying them before they occur. This can be accomplished through thorough monitoring of all users' activity across multiple systems and networks. If you notice any suspicious activity, contact your IT department immediately so that steps can be taken to prevent any further damage from occurring. When it comes to protecting against these types of threats, organizations should focus on two primary areas: detection and prevention. Detecting a breach early is crucial because most successful attempts at impersonation involve some level of social engineering which means there is often plenty of time between when someone becomes aware that something is not right and when a true threat has been established. For example, if a customer service representative gets a call from someone claiming to be their CEO asking for information about sensitive company operations, there should be ample time to detect what is happening without endangering sensitive data or systems. Most enterprises utilize various toolsets designed specifically for detecting different forms of impersonation attacks; however, no single solution is perfect in its ability to identify each type of threat that might come along.

2.4. Inference Attack. An inference attack targets a private key. The attacker searches for values in memory that correspond to unused parts of data stored on a blockchain and then tries to reverse engineer that data. If successful, an attacker would learn how a user created their private key and could potentially use it to steal funds from other users. It is important to note that most sophisticated malware is able to complete brute force attacks by themselves (i.e., without help from humans). This is possible because passwords are often stored as weakly encrypted SHA-1 hashes on devices running older versions of Android, so an Android device can simply guess every possibility until it finds one that works. Therefore, an attacker does not necessarily need access to memory in order to perform an efficient brute force attack. Even if there were no leaks at all, attackers might be able to discover some blockchains' password algorithms just by looking at them. For example, they could analyze a blockchain's source code or study common implementations of its hash function. If they find enough information about a certain type of hash function—such as its inner workings or common uses—they may be able to reverse engineer that function. For example, if they know both an encryption scheme and its hash value, they can figure out what data was used to generate it. That way, even if your private key is never exposed through a leak or bug, attackers may still be able to guess it with enough time and effort. To protect against inference attacks, always use key stretching. Key stretching involves using a slow hashing function to create many different hashes from a single input. You can read more about it here. In addition, you should use salt when creating keys instead of only using passwords alone. Using salt prevents attackers from using precomputed tables of prehashed passwords to crack new ones faster than normal brute force methods allow. You can read more about salts here. Lastly, you should always store private keys on isolated machines that are not connected to any networks while they are being generated or used. This ensures that if an attacker compromises your machine during generation or usage, he will not be able to steal those keys once you move them off the machine after completion.

2.5. Denial of Service on the Cloud. Denial of service attacks is generally associated with malicious intent. These types of attacks render networks unusable for users by creating a flood of packets in order to shut down important resources like DNS servers or HTTP web servers. On cloud services, denial- of service (DoS) attacks are generally aimed at shutting down or crashing servers and network infrastructure such as firewalls. These types of DoS attacks may be carried out by one or more attackers, but they can also be launched without direct human intervention. Automated systems may launch their own DoS attack if they become infected with malware that is programmed to carry out these tasks. In addition, some forms of ransomware cause similar effects as DoS attacks by taking over devices and using them to overwhelm target computers with requests. While there are no current reports of widespread DoS attacks against cloud providers, it is possible that we will see an increase in these types of incidents in 2017. In fact, it is likely that we will see an increase in many kinds of cyberattacks next year because hackers will have plenty of new opportunities created by advances in technology and because security teams will have less time to prepare for them. As more businesses move toward digital transformation initiatives next year, it is likely that we will see an increase in cyberattacks targeting both data centres and cloud environments. Cloud computing has already proven to be a tempting target for criminals who want to steal sensitive information or hold companies hostage with ransomware. As businesses continue to shift their operations online, criminals will continue looking for ways to exploit weaknesses in cloud infrastructures. This means that IT professionals need to pay close attention not only to what is happening inside their organizations but also outside of them—especially when it comes to threats posed by other companies' clouds. To make matters worse, there has been little done so far about improving security across clouds themselves; most efforts thus far have focused on securing individual clouds rather than addressing problems that affect all cloud environments equally. Thus, it seems likely that cloud vulnerabilities will grow even larger in 2017. It is important to note that while DoS attacks can be damaging and disruptive, they are typically considered nuisance attacks unless used as part of a larger scheme. For example, while you might get locked out of your Gmail account temporarily due to someone launching a DDoS attack against Google's servers (which happened recently), you probably will not suffer any long-term consequences from being unable to access your email for a few hours. However, suppose your business relies heavily on cloud services for day-to-day operations, and you lose access to those services because of an ongoing DDoS attack or another type of cyberattack. In that case, a user could suffer serious financial losses, a damaged reputation, and loss of customer trust.

2.6. Availability Attack. This attack is used to gain unauthorized access to a computer or network. The attacker enters using a backdoor, which can be done through telnet, ssh, FTP service, insecure wireless connections, or by guessing passwords. For example, an attacker might impersonate one of your employees in order to gain sensitive information from another employee. They could then use that information for more attacks or sell it to other hackers for money. To prevent availability attacks, employ firewalls and make sure your company's computer network does not have any open ports. It also helps to not use telnet as a method of remote access and password protect all devices connected to your network. If you do suspect you have been hacked, change all your passwords immediately. A man in Italy was arrested after attacking his local power grid and disabling electric service to 15 million people in Northern Italy. This was reportedly accomplished with only a few hundred dollars worth of equipment he bought online, including cables and small circuit boards known as smart plugs. He claimed he wanted to highlight security vulnerabilities at power plants across Europe. These types of cyberattacks are becoming increasingly common and difficult to prevent because they do not require specialized knowledge or training; anyone with basic Internet skills can execute them with little effort. One way you can minimize your chances of being targeted is by strengthening security around high-risk areas like power grids, so potential attackers know they will not succeed if they try something.

3. Detection Mechanisms for IoT-Based Security Attacks

An insight into detection mechanisms for IoT-based security attacks. The most common mechanism for detecting an attack is signature-based antivirus (SBAV). SBAV uses malware signatures, which are defined in advance for each type of known malware, to detect malicious software. However, due to a high rate of infection from unknown or zero-day exploits, it is a reactive method. It requires an organization to keep its AV signatures up to date with new threats. In addition to that, it is effective against traditional computer viruses but not equally effective when dealing with other cyber threats like smartphone viruses or zero-day attacks as it does not find any new vulnerabilities. As such, it is not very useful in protecting devices. Another approach used by organizations is whitelisting; rather than blocking applications, whitelisting only allows trusted applications to run on systems. This approach has proven useful for preventing users from running arbitrary programs; however, if attackers can successfully exploit a vulnerability before whitelisting can be updated, then they may still be able to run arbitrary code without being detected by antivirus software. Whitelisting also does not protect against rogue hardware since all hardware must be preapproved before use.

To overcome the problem of DoS and DDoS attacks, the author [15] proposed a simple but efficient DoS and DDoS attack for energy consumption, presented an effective method to defend against nonce value, and then proved by example it works. The authors present a very comprehensive survey with theoretical analysis research on various authentication methods to improve security levels, especially in terms of first-phase security detection or target identification. In addition, it points out that secure key management for providing sustainable service support is important. Recently many papers have been published related to two aspects of detecting DDoS attack technologies. A few papers focused on highly secure channel establishment from source server-side, which can effectively improve attack traffic tamper by time stamp mechanism with AES algorithm at layer 3 packet header field.

Another problem with securing IoT devices [16] is that each node in a network, including individual sensors or actuators, has its own unique IP address. However, instead of using a centralized gateway to process traffic, sensor nodes should be connected to a disaggregated SDN-enabled gateway that uses flow-based security rules (FBS). Such an approach is similar to how SDN can be used to secure wireless access points (APs) against DDoS attacks, where bandwidth management allows for users with malicious intent to consume available bandwidth quickly. Such management can also prioritize or block traffic to or from certain device categories by limiting available bandwidth accordingly. For example, when several thousand smart meters are deployed to measure energy consumption at different locations in a city, FBS could prioritize traffic from smart meters by monitoring utility company buildings to ensure they have sufficient bandwidth to send data back to base stations it can be processed. In addition, FBS could block any other type of communication [17] between these meters and other types of devices because such communications might indicate an attack. Similarly, if there are thousands of smart water meters deployed throughout a city collecting data about water consumption at different locations and sending it back to base stations for processing, FBS could prioritize traffic from these meters over other types of communication because their ability to send data is critical for keeping track

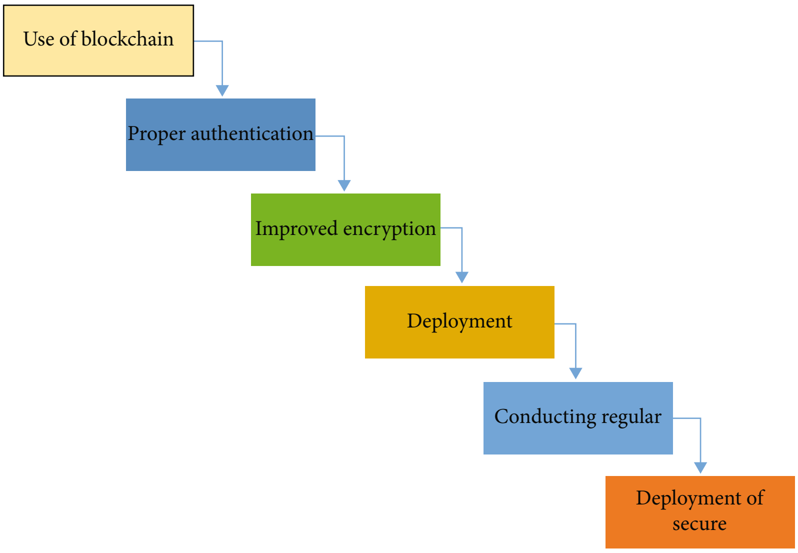

Figure 3: Prevention mechanism for IoT-based security attacks.

of water consumption. As a result, resources can be efficiently allocated to protect important parts of a network without having to rely on strict firewall rules and without having to use VPN technology [18] which creates latency and increases costs. Similarly, with proper use of FBS, VPN technology could even be eliminated entirely for noncritical data transfer since all IoT traffic would only need protection against DoS attacks; i.e., if not critical, then just drop it. With respect to prevention, once an attacker succeeds in hacking into one part of a system (i.e., one piece of hardware) [19], they will typically attempt to hack into another component as well; i.e., start at point A and then go toward point B until successful.

4. Prevention Mechanisms for IoT-Based Security Attacks

To overcome the problem of security attacks in Internet of Things (IoT), it is essential to use prevention mechanisms against attacks, such as firewalls. According to existing solutions, some intrusion detection systems (IDS) can identify firewall rule violations and therefore detect unauthorized traffic that could affect a company's infrastructure. However, most proposed approaches have not been tested using real data from open and closed networks, with different types of flows (TCP/UDP) whose rates vary over time. To fill these gaps, we propose an effective solution for detecting those violations through IDSs by designing static policies based on behavioural analysis rules to detect attack patterns requiring special system modifications. However, the subsections are below, while the flow chart is shown in Figure 3.

4.1. Use of Blockchain Technology. Blockchain technology has several properties that make it an excellent candidate for protecting Internet of Things (IoT) devices. The major one is its ability to store large amounts of data using cryptographic hash functions securely. In addition, blockchain networks are decentralized and anonymous, making them difficult to compromise. This ensures that every node in a blockchain network can perform any operation without letting other nodes know its identity. Moreover, once a new record is stored in a blockchain network, it cannot be modified or deleted; thus, records stored in blockchain remain immutable even when compared with other distributed ledgers such as those provided by Google File System (GFS) or MongoDB. To our knowledge, no studies have addressed how these characteristics can be used to prevent attacks against IoT devices. Therefore, we propose a novel approach based on blockchain technology to provide security guarantees for IoT devices. Specifically, we use smart contracts to create rules about how messages received from sensors should be processed by actuators and how sensors should send messages to actuators. We also use smart contracts to ensure that only authorized parties can add/delete/modify sensor records from/in blockchains. Finally, we also propose solutions for securing communication between sensors and actuators at runtime via encryption algorithms such as AES-CTR or ChaCha20-Poly1305. We implemented our proposed solutions in NodeJS and deployed them onto an ESP8266 board connected via MQTT protocol with AWS IoT cloud platform running on Amazon EC2 instances.

Blockchain is ideal for achieving data integrity and confidentiality because it consists of an append-only, shared ledger that includes cryptographic hashes. Similarly, existing cryptographic protocols are easy to deploy in a blockchain context, which makes them more appropriate for IoT networks than public key cryptography solutions (e.g., TLS). To overcome the problem of scalability and privacy protection in blockchain, we propose a solution to enable the secure sharing of information within a private environment among trustworthy nodes through homomorphic encryption [20].

As stated earlier, many studies have investigated how to improve trust between devices using both blockchain technology [21] and traditional trusted methods such as certificate authorities [22]. Still, others provide mechanisms for incentivizing correct or desired behaviour among peers [23]. However, these approaches do not directly tackle information sharing security problems or are not intended to be used for microservices. For example, Beaumier and Kalomeni [24] describe a framework where different entities operate microservices by combining a platform as a service element like Amazon web services with an Ethereum infrastructure. To date, no work has proposed mechanisms to protect sensitive information during interactions between particular IoT devices something required in most applications.

4.2. Proper Authentication and Tokenization. Proper authentication is paramount to building a secure, trustworthy system. Every IoT device must be authenticated using industry-standard protocols such as 802.1x (EAP), RADIUS, or OTP/CHAP. Once authenticated, devices must either use a dedicated secure protocol over TLS to communicate with their corresponding gateway, or their traffic should be properly encrypted within their protocol stack to ensure all communications are confidential and can only be decrypted by authorized parties. Additionally, these devices should never send sensitive information in clear text during communications between them and their corresponding gateway or other devices in order to prevent snooping attacks from hackers who may leverage collected data for malicious purposes such as account takeover.

In recent years, digital payment systems have become an integral part of our daily lives. Systems such as PayPal, Venmo, Google Wallet, and Apple Pay utilize authentication protocols in order to verify users' identities and safeguard sensitive information [25]. This paper explores use cases for multiple popular protocols, including OAuth 2.0, OpenID Connect, JWT (JSON Web Token), UMA (user-managed access), and SAML (security assertion markup language). It also compares their effectiveness based on a number of factors, including interoperability with other applications. While each protocol is effective in certain scenarios, UMA appears to be superior in most areas. For example, it can easily be implemented alongside any application or website and does not require additional hardware or software to function properly.

4.3. Improved Encryption Methods. In addition to improving encryption methods, engineers can take advantage of a number of emerging hardware features, including those designed to help prevent security breaches. For example, various implementations of silicon root-of-trust are intended to provide hardware authentication and digital signing capabilities. These techniques could protect against malware attacks that seek to steal secrets or inject false data into a system. Another such feature is Intel's Software Guard Extensions (SGX), which helps prevent software from being snooped upon or altered when it is running inside a processor. The SGX essentially creates an isolated sandbox for each application so that if one gets hacked, there is little risk it will negatively affect other processes in use at that time. Some types of processors also offer built-in protection against side channel attacks by using design features that make it harder for hackers to figure out what they are doing with all that computing power. Side channels refer to how malicious code taps into all sorts of sensors embedded in devices—such as cameras, microphones, and GPS receivers—to discover information about their environment without alerting users. Other new technology uses fog computing instead of relying solely on cloud storage. Instead of having all your sensitive data stored far away from you on some distant server farm somewhere else in cyberspace, fog computing stores it locally but connects you remotely through a secure connection to retrieve it when needed.

4.4. Deployment of Powerful Firewalls. Firewalls are an important element in any computer network. They are used to prevent unauthorized access to or from a private network. Another usage is to prevent a private network from being accessed by an unauthorized user (like in a distributed denial of service attack). If a firewall is deployed incorrectly, then it will be vulnerable to attacks. The firewalls should have their logs monitored continuously so that if there is any breach, it can be identified quickly. In addition, firewalls should have strong authentication methods for users so that even if there is a breach in the firewall, no damage can be done. Strong passwords are highly recommended for all administrators and users with access to firewalls.

4.5. Conducting Regular Security Vulnerability Assessment. After an attacker gains access to a system, they often remain undetected for long periods of time, using that access as a launching point for additional attacks. Similarly, keeping track of updates related to your software and hardware is important for minimizing security vulnerabilities. A lack of security testing can leave you vulnerable as new threats emerge or even after basic information security practices have not been followed. In order to detect vulnerabilities in your systems before an attacker does, it is imperative that you conduct regular vulnerability assessments. You should also be sure to keep up with updates on all devices or applications used by your organization. If you use IoT devices, there are many different ways that they could be attacked. For example, attackers could monitor network traffic from IoT devices in order to steal sensitive data or infect other connected computers. To prevent these types of attacks, make sure that IoT devices are regularly updated with firmware patches and ensure proper encryption protocols are being implemented. Additionally, consider implementing end-to-end encryption so only authorized users have access to sensitive data stored on these systems.

4.6. Deployment of Secure IOT Infrastructure. As with any new technology, IoT security breaches are a common occurrence. A recent research report by Centrify found that as many as 40% of all IoT deployments have critical security issues. A secure IoT network deployment requires diligence on multiple fronts, including authenticating hardware devices, protecting data in transit, and ensuring access controls are in place. If possible, deploy an encrypted virtual private network (VPN) such as IPsec to encrypt communication between endpoints and applications in order to prevent potential hackers from intercepting sensitive information such as credit card details. Use authentication tools such as RSA SecurID or Microsoft's Active Directory Identity Service for added protection against unauthorized access or malicious attacks. Deployment of proper identity management is essential to protect your customers' privacy and ensure they feel safe using your services. Be sure to also set up strong access control measures, including multifactor authentication, so only authorized users can access your system. This will help mitigate the risk posed by external threats such as phishing scams that rely on stolen credentials to carry out their attack. When it comes to deploying IoT infrastructure, it's important to think about both traditional IT security best practices as well as specific challenges posed by an Internet-connected device. To be effective, you need to consider things like how you will identify each device uniquely and how you can keep track of them over time. It would help if you also considered how you plan on updating software in a timely manner when vulnerabilities are discovered. It may be wise to invest in tools that make it easier for administrators to manage large numbers of IoT devices without having expertise in every single one. For example, companies like Cisco offer powerful systems for managing large-scale deployments through features like centralized administration, automated patching, and inventory tracking capabilities.

4.7. Proper Connection to the Cloud. The cloud is a critical aspect of IoT security, but it is also an enormous risk. While most cloud services are supposed to have secure firewalls, recent attacks have proven that these firewalls are not perfect. The most famous example is probably Mirai, a DDoS botnet that infected smart fridges, CCTV cameras, and other Internet-connected devices. It was created by exploiting some serious vulnerabilities in webcams from popular manufacturers. To keep your IoT network safe, you need to make sure all your devices are properly connected to your local network and not directly linked to public networks like Wi-Fi or Bluetooth. That way, you can ensure they do not get hacked via a remote connection. To make sure everything is working correctly, test your connection at least once every month or two. You can do so with an app like Fing (Android) or Netcut (iOS). Just type in public IP into Google before you start testing; otherwise, you might end up cutting off your own Internet access!

5. Specific Protection Technologies for Specific IoT Devices and Services

IoT security attacks are commonly framed as vague, futuristic threats, but they are already here. Vulnerabilities in connected devices have been used to take down critical national infrastructure, attack government agencies, facilitate international espionage campaigns, and steal sensitive medical data. A variety of cybersecurity technologies are currently being deployed (or planned for deployment) by various companies hoping to protect these increasingly valuable assets from such attacks. However, it is important to remember that no one solution will work for every situation—different protection technologies are necessary for different kinds of devices, services, and networks. Therefore, we need a thorough understanding of how each technology works before being able to determine its usefulness in preventing IoT-based security attacks. This survey provides just such an overview. It covers all major security technologies relevant to IoT devices and services, providing a detailed explanation of their functions and capabilities. The survey also includes an extensive collection of real-world examples illustrating how specific technologies were applied or could be applied in practice. Every type of device, service, and communication technology presents its own security vulnerabilities. In order to better protect our homes from Internet-connected devices, we need a better understanding of how these technologies are designed, how they work together, and how they can be used in malicious ways. We will take a detailed look at specific IoT-based attacks that were developed by testing security vulnerabilities on real devices. The main goal is to help companies identify common IoT vulnerabilities in their own hardware or software so that they can take steps toward fixing them through new product releases or patches. At least 20% of organizations will have been breached by IoT malware by 2020; let us all try our best to avoid it!

6. IoT Security Testing Standards and Tools

Rapid technological advancement makes IoT security testing tools available to help identify risks in IoT ecosystems. In a report from Northeastern University, researchers say that identifying cybersecurity problems will require standards for evaluating devices and software. There are standards for what is known as cyber physical systems combinations of computers and physical devices like those used in manufacturing plants, but there are few widely accepted standards for analyzing software used by sensors, which make up a large part of an IoT ecosystem. Without such standards, according to Jessica Groopman, an associate professor at Harvard Medical School who studies medical device security, the challenge is that you really do not know if your system was properly tested. If a manufacturer has not conducted proper penetration testing, it could mean that their product is vulnerable to attack.

IoET research suggests that cybersecurity testing should be an integral part of IoT product development. In fact, security testing is recommended by a number of government agencies, including in both Canada and the United States. The Canadian government recommends each device developer follow a checklist that includes evaluation by penetration testers using tools like Kali Linux or Burp Suite. Similarly, US governmental agency NIST recommends penetration tests with tools like Metasploit or SET as part of its guidelines for evaluating devices. And according to recent research from Northeastern University, these recommendations are supported by standard bodies such as ISO/IEC JTC1 SC27 WG5 and IEEE P2413. Unfortunately, it is hard to know if any specific manufacturer has conducted proper testing because there are no widely accepted standards for evaluating IoT products. It is not clear whether any of these organizations have conducted their own independent tests on products sold in stores today, but it seems likely that they have at least evaluated some of them since they all recommend security evaluations before launch.

The most comprehensive report on IoT attacks comes from researchers at Symantec, who reviewed over 10 million attack attempts against more than 100 companies across various industries between 2015 and 2017. They found that 99% of all attacks were focused on one of three things:

These attacks aimed to install malware or steal data by gaining access to a corporate network, with criminals attempting to compromise an organization's security to gain access. Attackers also frequently used botnets, groups of infected computers controlled remotely by hackers, to conduct distributed denial of service (DDoS) attacks which flood a website with traffic until it crashes—and brute force password guessing in order to gain access into corporate networks. Another common tactic is for attackers to use phishing emails containing malicious links or attachments that can give them control over a victim's computer once they click or open it.

7. Challenges in Detection and Prevention

IoT is undoubtedly an exciting technology that promises great possibilities but also presents new security challenges. Incidents have been growing steadily as IoT-based attacks continue to gain ground. A recent study shows that enterprises will spend between $2 billion and $6 billion on IoT security in 2017 alone. Understanding where attacks are likely to occur remains critical for prevention. For example, software security issues often reside in applications that run on connected devices. It follows then that protecting them becomes a top priority in preventing breaches. However, data centres also remain vulnerable, especially when they contain several types of connected devices being controlled remotely via different protocols. Malware can spread quickly across devices if not properly configured. In addition, there is still plenty of work to be done in terms of securing communications between connected devices. The key lies in deploying IoT security solutions capable of identifying threats early on and mitigating them before they cause damage. With proper planning and execution, we can significantly reduce incidents related to malware infection, DDoS attacks, botnets, unauthorized access, or control over sensitive information. On another note, IoT has made it easier than ever to launch large-scale attacks. Indeed, most organizations do not have sufficient resources to monitor billions of sensors worldwide 24/7. This means monitoring tools must detect anomalies in network traffic patterns and automatically correlate events from multiple sources. This is particularly important because attackers may try to hide their tracks by modifying traffic or hiding inside encrypted traffic streams. Organizations need proactive detection mechanisms to effectively prevent IoT-related security breaches that can identify anomalies regardless of whether attackers use standard or nonstandard ports or protocols. Finally, one of IoT security's biggest challenges is ensuring users take appropriate precautions. While many users are aware of common security risks, such as phishing scams and password hacks, others seem oblivious to potential threats. There is little doubt that education needs to play a significant role in reducing incidents related to human error—for instance, forgetting to change default passwords on connected devices or clicking on malicious links sent via email. Criminals will continue using these methods with relative impunity if users fail to recognize common cyberattacks. Ultimately, IoT security comes down to three things: (1) taking preventive measures to minimize risk, (2) using effective detection systems [26, 27] to catch threats early, and (3) educating users about best practices. Organizations can better secure themselves against IoT-based attacks by combining these three elements. At a minimum, IoT security plans should include regular updates to existing connected devices and constant monitoring of incoming traffic. Beyond that, organizations should seek out security solutions that can mitigate attacks in real-time and make it easy to detect anomalies without adding too much overhead.

8. Finding a Solution to IoT Security Threats

As IoT connected devices like smartwatches, refrigerators, and even our cars become more sophisticated with rich features, there is a greater need for security. It is not easy to detect if an IoT device has been compromised. It is essential that users are aware of IoT security threats to prevent any sort of loss due to cyber criminals using their smart gadgets against them. IoT manufacturers should focus on providing a secure experience for their customers by integrating preventive measures such as firewalls, VPNs, and encryption methods, into their products. Also, users must take extra care when connecting their devices to other network services over the Internet. This would help in preventing unauthorized access from hackers. If a user suspects their device or service is being hacked, they can disconnect it from the Internet immediately and then change passwords to regain control over it.

One of the most popular methods of detecting attacks is creating honeypots (honeynets). Honeypots mimic real-world systems and entice attackers who think they are accessing real assets online or via wireless communication networks. The idea behind honeypots is simple—if you want to know what people are doing, set up something that looks interesting enough so they will come to play with it and do something interesting so you can observe what they do when they get there. A user needs a lot of knowledge about hacking techniques to create a proper honeypot.

You do not need a complex solution if your goal is to detect if someone has accessed your system without your permission. Many free tools on the Internet let you detect if someone has logged into your account from an unknown location. For example, Google Alerts lets you monitor specific queries across more than 50 search engines, including Google News and Google Groups. You can also use Hootsuite or TweetDeck for monitoring social media activities. These tools will alert you when someone mentions your brand or username in their posts. You can set up alerts for keywords that hackers might use and words that indicate malicious activity like hacked and cracked. This way, you will be able to know about any suspicious activity happening online related to your brand and take action accordingly.

Protecting IoT devices is not an easy task. If manufacturers do not take proper measures from inception, it will be impossible for users to detect any breach. Even if you have a firewall in place, you can never be sure about its effectiveness because attackers are always looking for vulnerabilities in your network that they can exploit. To prevent attacks on your network, you must ensure that there are no unnecessary ports open on your device that hackers could use. Use strong passwords that contain uppercase letters, lowercase letters, numbers, and special characters with a length of at least 10 characters. However, passwords are straightforward to guess, so making them complicated worsens things. It is better to use two-factor authentication (2FA), which requires you to enter a code sent via text message or email every time you log into your account. This way, even if someone guesses your password, they will not be able to access your account without having access to your phone or email account. Then, the user should also change all default passwords associated with IoT devices such as wireless routers and modems immediately after purchasing them from stores.

If possible, try changing the default SSID name of the wireless router and disabling the SSID broadcast option so that other people cannot connect easily without knowing the exact name of the wireless network.

9. Conclusion and Future Work

This survey has covered a lot of ground. We first discussed some of the fundamentals behind IoT security before discussing practical detection strategies that are currently used. Then, we moved on to discuss future challenges in terms of prevention. There are still plenty of opportunities for future work. Both detection strategies, as well as countermeasures, can be extended or improved further. One area could be merging several existing solutions into a more robust solution. Another direction is exploring new ways to detect attacks with different techniques such as anomaly-based approaches. Other possibilities include extending our current analysis to different types of attacks, such as insider threats or side channel attacks. The last direction is investigating potential hybrid approaches that combine multiple detection methods. In conclusion, there is no doubt that IoT will continue to grow rapidly in both number and complexity, which means there will be plenty of opportunities for security researchers and practitioners alike.

Data Availability

No data is available.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This work is supported in part by the Guangdong Province Key Research and Development Plan (Grant No. 2019B010136003), the National Natural Science Foundation of China (61902082), the Guangdong Higher Education Innovation Group (2020KCXTD007), and the Guangzhou Higher Education Innovation Group (202032854).

References

[1] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, “Cyber security in IoT-based cloud computing: a comprehensive survey,” *Electronics*, vol. 11, no. 1, article 16, 2022.

[2] S. Anwar, Z. Inayat, M. F. Zolkipli et al., “Cross-VM cache-based side channel attacks and proposed prevention mechanisms: a survey,” *Journal of Network and Computer Applications*, vol. 93, pp. 259–279, 2017.

[3] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “CorrAUC: a malicious Bot-IoT traffic detection method in IoT network using machine learning techniques,” *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2021.

[4] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city,” *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[5] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “IoT malicious traffic identification using wrapper-based feature selection mechanisms,” *Computers & Security*, vol. 94, Article ID 101863, 2020.

[6] S. Weisman, *What Are Denial of Service (DoS) Attacks? DoS Attacks Explained*, Norton Lifelock, United States, 2020.

[7] H. Hasbullah, I. A. Soomro, and J. L. Ab Manan, “Denial of service (DOS) attack and its possible solutions in VANET,” *International Journal of Electronics and Communication Engineering*, vol. 4, no. 5, pp. 813–817, 2010.

[8] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, “Detection and mitigation of data manipulation attacks in AC microgrids,” *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2588–2603, 2020.

[9] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, “Anomaly detection in automated vehicles using multistage attention-based convolutional neural network,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291–4300, 2021.

[10] S. Shukla, S. Thakur, and J. G. Breslin, “Anomaly detection in smart grid network using FC-based blockchain model and linear SVM,” in *International Conference on Machine Learning, Optimization, and Data Science*, pp. 157–171, Springer, Cham, 2021.

[11] A. Chehri, I. Fofana, and X. Yang, “Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence,” *Sustainability*, vol. 13, no. 6, article 3196, 2021.

[12] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, “Federated-learning-based anomaly detection for IoT security attacks,” *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2022.

[13] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, “Improving Internet of Things (IoT) security with software-defined networking (SDN),” *Computers*, vol. 9, no. 1, 2020.

[14] WireShark, “Trace traffic WireShark,” 2015.

[15] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, “Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: an experimental approach,” *Sensors*, vol. 20, no. 3, 2020.

[16] 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)*, pp. 157–163, Vienna, Austria, August 2016.

[17] H. Zhang, G. Lu, M. T. Qassrawi, Y. Zhang, and X. Yu, “Feature selection for optimizing traffic classification,” *Computer Communications*, vol. 35, no. 12, pp. 1457–1471, 2012.

[18] J. A. Donenfeld, “WireGuard: fast, modern, secure VPN tunnel,” Black Hat, USA, 2018.

[19] H. Abbasi, N. Ezzati-Jivan, M. Bellaiche, C. Talhi, and M. R. Dagenais, “Machine learning-based EDoS attack detection technique using execution trace analysis,” *Journal of Hardware and Systems Security*, vol. 3, no. 2, pp. 164–176, 2019.

[20] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, “IoT information sharing security mechanism based on blockchain technology,” *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.

[21] L. Wu, X. Du, W. Wang, and B. Lin, “An out-of-band authentication scheme for Internet of Things,” in *2018 International conference on computing, networking and communications (ICNC)*, pp. 769–773, Maui, HI, USA, March 2018.

[22] J. Chaudhry, K. Saleem, P. Haskell-Dowland, and M. H. Miraz, “A survey of distributed certificate authorities in MANETs,” *Annals of Emerging Technologies in Computing*, vol. 2, no. 3, 2018.

[23] M. D. Sánchez-Hernández, M. C. Herrera-Enríquez, and F. Expósito, “Controlling behaviors in couple relationships in the digital age: acceptability of gender violence, sexism, and myths about romantic love,” *Psychosocial Intervention*, vol. 29, no. 2, 2020.

[24] G. Beaumier and K. Kalomeni, “Ruling through technology: politicizing blockchain services,” *Review of International Political Economy*, pp. 1–24, 2021.

[25] G. Thawre, N. Bahekar, and B. R. Chandavarkar, “Use cases of authentication protocols in the context of digital payment system,” in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, Kharagpur, India, July 2020.

[26] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, “Data mining and machine learning methods for sustainable smart cities traffic classification: a survey,” *Sustainable Cities and Society*, vol. 60, p. 102177, 2020.

[27] M. Shafiq, X. Yu, A. K. Bashir, H. N. Chaudhry, and D. Wang, “A machine learning approach for feature selection traffic classification using security analysis,” *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4867–4892, 2018.