Survey on Risks Cyber Security in Edge Computing for The Internet of Things Understanding Cyber Attacks Threats and Mitigation

Tiara Rahmania Hadiningrum [1)], Resky Ayu Dewi Talasari [2)], Karina Fitriwulandari Ilham [3)], and Royyana Muslim Ijtihadie [4,*)]

[1, 2, 3, 4)] Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

E-mail: 6025231079@student.its.ac.id[1)], 6025231019@student.its.ac.id[2)], 6025231056@student.its.ac.id[3)], and roy@if.its.ac.id[4)]

ABSTRACT

In the era of rapid technological development, the use of IoT continues to increase, especially in the context of edge computing. This survey paper thoroughly explores the security challenges that arise in the implementation of IoT at the edge computing level. The focus of this research is the potential cyber attacks and threats that can affect system security. This paper identifies cybersecurity risks that may arise in an IoT environment at edge computing through the literature survey method. The research methodology approach is used to classify attacks based on their impact on infrastructure, services, and communications. The four classification dimensions, namely Network Bandwidth Consumption Attacks, System Resources Consumption Attacks, Threats to Service Availability, and Threats to Communication, provide a basis for understanding and addressing security risks. This paper is expected to provide a solid foundation of understanding of security in IoT in edge computing, as well as a contribution to the development of effective security strategies. By focusing on an in-depth understanding of security risks, this paper encourages the development of future adaptive security solutions to address security challenges that evolve with the rapid adoption of IoT technologies in edge computing.

Keywords: Cyber security, cyber attack, cyber threat, IoT, edge computing

1. Introduction

With the rapid development of the technological era, the use of Internet of Things (IoT) devices is increasing. IoT is a global network that connects smart devices and other physical objects equipped with sensors and software to collect, transmit, and process data [1]. The implementation of IoT can help devices interact automatically so that interactions between devices are more effective and coordinated [2]. Due to its advantages, the application of IoT is increasing in various fields such as smart vehicles, smart buildings, smart homes, and smart healthcare [3].

The process of transmitting data from IoT devices to data processing infrastructure, such as data centers or cloud computing is important [4]. However, the implementation of this process raises several issues, including increased latency time in data ingestion and increased operational costs. Challenges related to data management, processing, and storage require complex technical approaches [3]. The proposed solution must comply with privacy, security, and regulatory standards to improve infrastructure performance and reliability. [5].

In the face of ever-evolving technological advances, the security aspect of IoT in edge com-puting is one of the most important things [6]. Especially in understanding the security risks associated with the implementation of IoT in edge computing, especially given the limited resources and close interconnection between devices in edge computing environments. [7], [8], [9]. In line with the rapid growth of IoT technology in various sectors, concerns about complexity and increasing penetration are the main cornerstones of this survey [10]. Therefore, security risk mitigation measures are something that cannot be ignored to improve the security of IoT implementations in edge computing.

* Corresponding author.
Received: December 22nd, 2024. Revised: February 11th, 2025. Accepted: February 16th, 2025.

Available online: February 25th, 2025.

DOI: 10.12962/j24068535.v23i1.a1210

The importance of mitigation is not only limited to reducing the risk of attacks and threats that can affect security. In the context of implementing IoT in edge computing, limited resources and close connection between devices are the main challenges, so mitigation is one of the things that can minimize attacks and threats. One of the mitigation efforts that can be done by controlling the configuration and operation of edge computing and implementing data encryption. Thus, mitigation is not only a response to risk, but as a proactive effort that can significantly reduce the chances of attacks and threats that may arise in edge computing [11].

This survey paper aims to present a comprehensive understanding of security attacks, threats, and mitigation strategies in the context of IoT in edge computing. Utilizing a literature survey method, this research explores the security characteristics that arise in the implementation of IoT in edge computing and analyzes the associated risks. The focus involves exploring various emerging attacks, such as those that impact bandwidth consumption, system resources, service availability and communication along with effective mitigation. Thus, it is hoped that this paper can provide knowledge in dealing with attacks and security threats on IoT in edge computing.

This survey paper is designed with an organized structure, starting with Section 1 which presents the background related to the IoT paradigm in edge computing. Section 2 discusses a survey of previous research that has addressed IoT in edge computing. Section 3 discusses the taxonomy used in the analysis of security and privacy attacks and threats for IoT in edge computing so as to provide a comprehensive analysis of security and mitigation issues in the context of IoT in edge computing. Section 4 focuses on the survey discussion that addresses the classification of attacks, threats and mitigations in the cybersecurity domain of IoT in edge computing, Section 5 provides in-depth analysis and discussion of the survey results, while Section 6 discusses the conclusions of the survey paper and offers future research directions.

2. Related Works

There are several surveys and research that have been conducted in academia regarding the security aspects of IoT in edge computing. However, it should be noted that exploring all aspects requires a considerable amount of research time. Therefore, we compiled this survey paper to review some related literature and research papers. Through the survey paper presented, it is hoped that this survey paper will be able to provide an understanding of the cybersecurity aspects of IoT in edge computing, making it easier for readers to gain a comprehensive understanding of topics related to security in IoT in edge computing.

The survey conducted by Alwarafy et al.[8] entitled “A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things” addresses security and privacy challenges in the IoT paradigm in Edge computing. The focus is to address the literature gap on IoT in edge computing. This survey paper provides an overview of further research that can be done on specific security and privacy challenges in IoT in edge computing, with additional performance evaluation, to improve the understanding and development of more secure paradigms. However, this paper provides less in-depth analysis of specific security and privacy issues and more overviews, attack classifications, and potential solutions. Performance evaluation of IoT-based security architectures in edge computing is also not discussed.

The survey conducted by Sha et al. [12] entitled “A survey of edge computing-based designs for IoT security” the authors present a comprehensive survey of existing IoT security solutions in edge computing and discuss IoT security in edge computing. The authors also analyze IoT security vulnerabilities in edge computing at various layers and present a comparison of new security schemes based on emerging solutions. In addition, this paper also proposes a security architecture that can be dynamically customized based on needs. However, this paper does not provide in-depth information on the practical implementation of the proposed security solutions in the context of edge computing. In addition, this paper discusses the effectiveness of the proposed security solutions in the context of edge computing.

In the survey paper written by Fazeldehkordi et al. [13] “A Survey of Security Architectures for Edge Computing-Based IoT”, the authors discuss various security aspects related to edge computing in the context of IoT and provide a comprehensive definition of edge computing and analyze various existing security solutions and

security challenges faced in the implementation of IoT in edge computing. In addition, this paper also proposes a security architecture that can be dynamically customized based on needs and presents various solutions and countermeasures to address security and privacy threats in the edge computing environment. However, there are some shortcomings, namely that this paper lacks focus on specific security solutions or algorithms used in the security architecture, does not discuss the privacy implications of the proposed security solutions and lacks in-depth information on the effectiveness and efficiency of the proposed solutions in addressing security and privacy threats in IoT-based computing environments.

The survey conducted by Kalariya et al. [14] "A Systematic Literature Review on Edge computing Security" is dedicated to exploring security issues in the edge computing domain. Specifically, it takes the form of a Systematic Literature Review (SLR), which aims to uncover the latest technologies and strategies designed to mitigate security threats in edge computing. Despite its comprehensive nature, this survey paper still does not provide specific technical implementations or real-world case studies that illustrate how the discussed security technologies and strategies can be applied in the context of Edge computing. In addition, this paper lacks an in-depth discussion of how edge computing differs from cloud computing in terms of security and their respective advantages. A more detailed exploration of practical implementations, case studies, and comparative analysis of security aspects between edge computing and cloud computing would enhance the contribution of this paper survey in understanding and addressing security challenges in the Edge computing domain.

In a survey conducted by Xiao et al. [15] yang berjudul "Edge computing Security State of the Art and Challenges" explores the context of security in edge computing by addressing attacks and defense mechanisms. While discussing the important role of IoT and smart devices in edge computing. The paper's survey emphasizes efficient solutions for IoT devices, but the paper does not describe security threats and only focuses on four main types of attacks namely Distributed Denial of Service (DDoS) attacks, side channels, malware injection, and authentication and authorization attacks.

Overall, the previous survey papers presented have some significant shortcomings, including the lack of in-depth analysis of specific security issues in IoT in edge computing that focus on overview and classification of attacks without providing detailed analysis, and the lack of understanding of the types of threats in IoT in edge computing. In addition, this paper chooses to focus on attacks, threats and mitigations in IoT in edge computing, so that this paper can provide more comprehensive and practical guidance on IoT security in edge computing.

From this gap, we would like to analyze more deeply the security issues in IoT in edge computing. This may include concrete examples to provide a better understanding. In addition, this survey paper will include consideration of possible attacks and threats on IoT in edge computing related to cybersecurity that are not covered in related papers. This can provide a more complete view of potential security risks and solutions.

In detailing the cybersecurity risks that may arise in the context of IoT in edge computing, a research methodology approach aims to understand the relevant attacks and threats. This methodology will form a solid foundation for identifying potential vulnerabilities and developing effective security strategies. Through a comprehensive survey, a series of cybersecurity risks that can affect IoT systems in edge computing are explored, allowing a deeper understanding of the complexity of security in IoT systems in edge computing. This classification process begins by identifying the types of attacks and threats that can occur in the context of IoT in edge computing, which are then arranged into a taxonomy that is grouped based on the aspects that can affect infrastructure, services, and communications in IoT in edge computing. Among them are attacks that can consume network bandwidth capacity, consume system resources, disrupt service availability so that it can hinder the normal functioning of services, and can disrupt the communication process in a network or system.

3. Methodology

Fig. 1 provides a visual representation of the four classification dimensions: network bandwidth consumption attacks, system resource consumption attacks, threats to service availability, and Threats to Communication. This

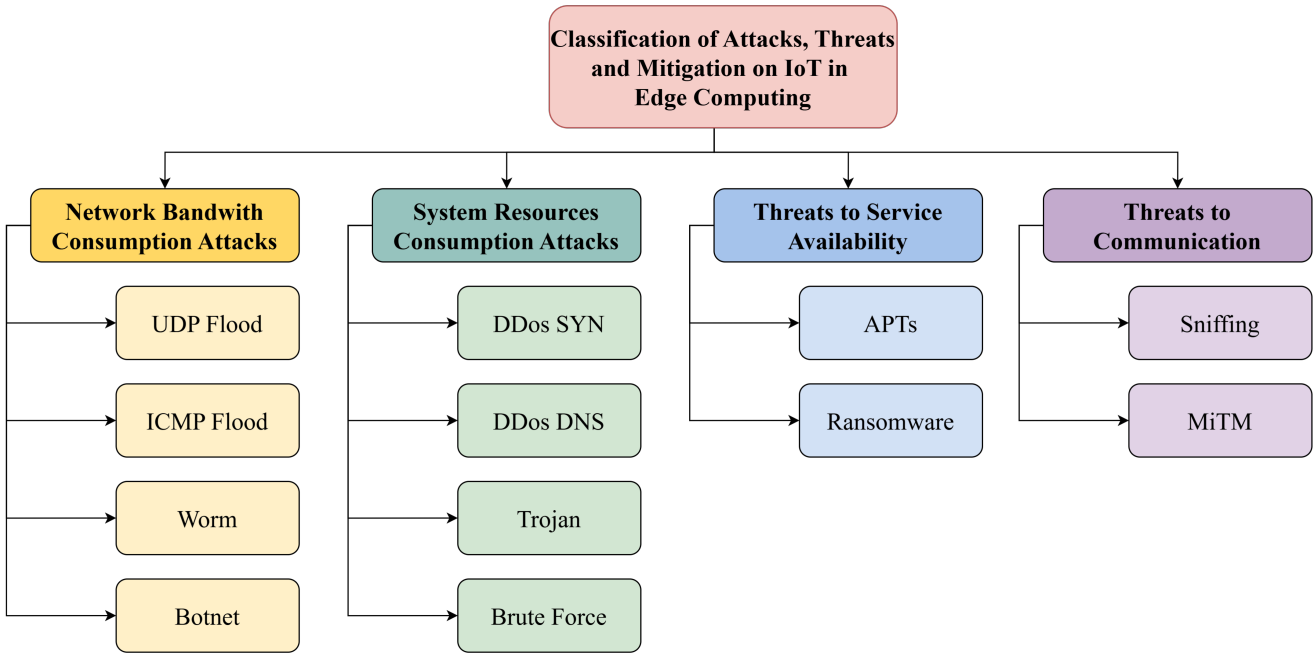

Fig. 1: Research Taxonomy

step not only provides a basis for categorizing attacks based on their characteristics but also helps build a deeper visual understanding. By separating attacks into structured groups.

First, the Network Bandwidth Consumption dimension considers parameters such as traffic patterns, frequency, and intensity of attacks. Attacks such as User Datagram Protocol (UDP) floods, Internet Control Message Protocol (ICMP) floods, Worms, and Botnets are grouped in this dimension based on their impact on network bandwidth capacity and efficiency. Second, the System Resources Consumption impact dimension considers indicators such as CPU, RAM, and storage usage. Synchronize (SYN) DDoS, Domain Name System (DNS) DDoS, Trojans, and Brute Force are categorized in this dimension based on how these attacks harm the availability and integrity of system resources. Third, the service availability threat dimension evaluates the attack strategy and the level of risk to the overall operations. Threats such as Advanced Persistent Threats (APTs) and Ransomware are placed in this dimension based on the potential of the attacks to damage and harm service availability. Finally, the communications threats dimension looks at how attacks threaten the integrity and confidentiality of data communications, and attacks such as Sniffing and Man in the Middle (MiTM) are classified based on these characteristics. Understanding and applying these criteria can be the basis for developing a more effective and responsive protection strategy against various types of threats in the IoT environment in edge computing.

Network Bandwidth Consumption in IoT in edge computing is an important element because it directly affects efficiency and security. When IoT devices operate with limited resources in an edge computing environment, managing bandwidth consumption wisely becomes the main thing in maintaining the availability of resources that are important for fast security response. Network overload caused by uncontrolled bandwidth consumption can be exploited by attackers launching attacks such as UDP flood, ICMP flood, worm, and botnet. By controlling bandwidth consumption, the risk of overload can be minimized, so that it can maintain network performance and availability in detecting, preventing, and responding to security threats. Therefore, managing bandwidth consumption also plays a role in improving the security and reliability of IoT systems in edge computing [16].

The importance of discussing system resource consumption attacks on the IoT in edge computing lies in its role in maintaining system security and performance. Threats of attacks that impact resource consumption, such as DDoS with the SYN flood method, DNS services, Trojans, and Brute Force can disrupt the operation of IoT devices that rely on limited resources in edge computing environments. Effective management of resource consumption is key to preventing potential threats to IoT data security and operations, as well as ensuring system availability and

responsiveness. With a deep understanding of these potential attacks, proactive steps in mitigating attacks and wise management of resource consumption can be an effective strategy for maintaining the reliability of IoT systems in edge computing environments. [11] [17].

In the study of [18] threats to Service Availability handling are also important. This is due to several main reasons. First, attacks that can damage service availability, such as APTs and Ransomware attacks, have a serious impact on the performance of edge computing systems and can cause problems for IoT devices connected to the system. Second, unstable service security can result in system failure and risk of use, thus threatening system performance and user satisfaction. Finally, when edge computing and IoT systems operate in an integrated manner, attacks that affect service availability can disrupt various applications and services that depend on the system. Therefore, understanding and addressing the threats that can disrupt service availability is essential to maintain the security and performance of edge computing in the context of IoT.

In the study of [19] threats to Communication in the context of IoT in edge computing must be discussed because they have a direct impact on system data communication. In the increasingly important edge computing architecture along with the development of IoT, secure and reliable communication between IoT devices and edge infrastructure is key to maintaining data integrity, avoiding potential attacks on malicious data, and ensuring smooth device operation. Threats to communication, such as attacks on the sensor layer, communication layer, and computing layer on the server, can disrupt vital data flows, threaten system security, and affect operational efficiency. Therefore, understanding and addressing threats to communication in the context of IoT in edge computing is essential to maintain system sustainability and security and maximize the benefits of this architecture.

4. Survey Discussion

A survey of 20 related papers revealed interesting findings around cybersecurity risks in the context of edge computing in IoT. The analysis of different types of cyberattacks provides insight into the challenges faced in protecting IoT in edge computing. This survey paper also discusses how previous research has responded to and addressed these risks. In this discussion, we also present issues in IoT in edge computing that have not been addressed by previous research, thus providing potential directions for the development of future security solutions. The results of this survey provide a more understandable view of cybersecurity in IoT in edge computing and provide an overview for further research in this area.

4.1. Network Bandwith Consumption Attack

Network Bandwidth Consumption Attack is an attempt to impede or damage network availability by increasing bandwidth usage excessively. In this attack, the attacker intentionally floods the target network with large data traffic, causing performance degradation and access disruption for legitimate users. Monitoring bandwidth usage on IoT devices in edge computing is critical as it has a direct impact on system performance and security. In the resource-constrained environment of edge computing, proper management of bandwidth utilization is essential to maintain the necessary resources in the face of security threats. Network overload caused by excessive bandwidth usage can be exploited by attackers carrying out attacks. Controlling bandwidth usage can reduce the risk of disruption and maintain stable network performance to protect IoT systems in edge computing. [16].

Bandwidth consumption attacks involve attacks that focus on over-utilizing network bandwidth, thereby causing network traffic to become inefficient and hindering communication between IoT devices and edge servers, reducing the available network capacity to transfer critical data. The impact is an increase in response time, a decrease in communication quality, and the potential for communication failures between devices, which can degrade the IoT system in edge computing.

A common method used in bandwidth consumption attacks involves sending a large number of fake requests or data packets to the target server and forcing the network infrastructure to work beyond its normal capacity. [20], [21]. This attack falls under the Denial of Services (DoS) and Distributed Denial of Services attacks (DDoS) [22]. Prevention efforts involve the use of firewalls, traffic anomaly detection with Intrusion Detection Systems and

bandwidth management to identify and respond to such attacks. The following are the types of attacks that disrupt Network Bandwidth Consumption on IoT infrastructure in edge computing.

A. UDP Flood

UDP flood is one of the most common types of DDoS attacks. It is carried out by sending a large number of UDP packets to the target, which can overload the network and make it unable to function properly. UDP flood attacks can be carried out easily because the UDP protocol does not require a stable connection and does not require verification of received packets. [23], The impact of a UDP flood attack is bandwidth saturation, which can result in normal services connected to the computer becoming inaccessible to authorized users [24]. UDP flood attacks are also utilized by Botnets that aim to create massive congestion that exceeds the capacity of network nodes and ports. By using UDP packets that have forged source addresses, the attackers make their victims crash due to high traffic volumes. These attacks can create instability on the network, which can harm IoT devices that are operating properly. It can cause IoT devices to not be able to function optimally [25].

In a study conducted by Bhardwaj et al. [26] overcoming UDP flood attacks by using a system with two main parts, namely edge functions and ShadowNet service, which is a service or system that acts as a dedicated server, this service is tasked with monitoring and analyzing shadow packets sent by edge functions. Edge functions are tasked with managing UDP data traffic by sending special packets called “shadow packets,” which are small data packets containing the word “shadow.” These packets are sent over the network at high speeds. These packets are sent over the network at high speed. When these shadow packets arrive at ShadowNet, their arrival time is recorded. The system then compares the arrival time of this shadow packet with the previous packet. This difference in arrival time tells the system about the speed of the data traffic. If the system detects that the shadow packets are arriving too fast, it indicates that a UDP flood attack may be taking place, and the system will immediately raise an alert. This helps in detecting and responding to attacks quickly. The results of this research are expected to improve the resilience and security of IoT systems against UDP flood attacks and illustrate the potential of edge computing in protecting IoT infrastructure from increasingly complex cyber threats.

Then research conducted by Nihri et al. [27] aims to develop a J48 algorithm-based Intrusion Detection System (IDS) to mitigate UDP flood attacks on IoT devices. The proposed solution to address UDP flood attacks includes four key aspects. First, real-time traffic monitoring allows the IDS to actively monitor traffic on IoT middleware devices. Therefore, the IDS is capable of early detection of anomalous patterns associated with UDP flood attacks. Second, the application of dynamic thresholds with an adaptive approach to changes in traffic patterns so that IDS can automatically detect accurately. Third, historical data-based attack pattern recognition to detect UDP flood attacks by identifying specific characteristics of traffic patterns.

Finally, rapid response after detecting an attack is an important aspect in risk mitigation efforts, with this IDS being able to take immediate action such as isolating the affected device or applying other protective measures to stop the attack quickly.

B. ICMP Flood

ICMP flood or ping flood is an attack that involves sending repeated ICMP echo messages from a victim computer with a spoofed source address. These messages are sent to broadcast addresses on the network, which allows messages to be sent to many devices at once. By utilizing fake source addresses, attackers can increase the frequency of ICMP echo messages and create a double effect called a DDoS attack. In a DDoS attack, attacks come from multiple sources simultaneously making it more difficult to handle [28].

In an ICMP flood attack, the attacker tries to exploit the ICMP protocol by creating an attack through sending many echo request packets to the edge computing as quickly as possible without waiting for a reply, resulting in a significant slowdown throughout the system. In addition, Transmission Control protocol (TCP) also triggers many SYN requests to edge computing by using fake IP addresses, while the server waits for ACK confirmation. This type of attack can cause the server to be overloaded and unable to operate normally and cause an overall decrease

in system performance. Therefore, it is important to identify and protect servers from these flooding attacks by implementing effective security measures and monitoring network traffic to detect suspicious attack patterns [29].

In research conducted by Yudhan et al. [30] presents a solution to overcome ICMP flood attacks using simulation experimentation methods on cloud and edge computing networks. The solution presented uses Packet Filtering Firewall and Circuit Level Gateway Firewall against ICMP flood DDoS attacks. This research also shows a comparison between before and after the ICMP flood attack with the Circuit Level Gateway Firewall. By applying Packet-Filtering Firewall successfully reduced traffic by 64%-69% and was able to reduce server resource usage by 73.75% and successfully returned traffic and crashed servers to normal conditions.

Research conducted by Jia et al. [28] also discussed solutions to deal with DDoS attacks on IoT including ICMP flood attacks using a defense mechanism called FlowGuard. FlowGuard is a defense mechanism based on edge computing and uses Machine Learning to detect DDoS attacks on IoT. Machine Learning to detect DDoS attacks on IoT. This research shows that FlowGuard is effective in identifying ICMP flood attacks and reducing the impact of DDoS attacks on IoT.

C. Worm

A significant problem that often arises in this era is the emergence of malicious software devices such as worms that have similar behavior to the same threats to operating systems, worms that have similar behaviors to the same threats to desktop operating systems [31]. Worms refer to a type of malware that can spread quickly through computer networks without user in-action. Worms can be used by cybercriminals to take over IoT devices, such as household routers, and utilize them for various malicious purposes [32]. Worm attacks can cause serious damage, especially to IoT devices in edge computing.

IoT worms work by spreading through computer networks and looking for vulnerable IoT devices to take over. After successfully taking over an IoT device, the worm can utilize it for various malicious purposes. IoT worms can spread quickly because IoT devices are often poorly protected and have security flaws that can be exploited by cybercriminals [32].

In research conducted by Yang et al. [33] discussed the vulnerability of sensor networks to worm attacks. The focus was on buffer-overflow vulnerabilities in the sensor program, where worms can exploit these gaps to infiltrate and spread to other sensor nodes. The biggest threat is that a single successful worm packet can compromise the entire sensor network. To improve security against these attacks, they also propose a software diversity approach which is an approach that suggests using different versions of software among the nodes. This way, if one software version is vulnerable to a worm attack, then not all sensor nodes will be affected as some nodes use different software versions. The research then provides analytical and simulation results to demonstrate the effectiveness of the proposed scheme.

D. Botnet

A botnet is a network of many bots designed to perform malicious activities on a target network. These botnets are controlled using command protocols and are controlled by a single entity called a botmaster [34]. Attackers conducting DDoS attacks tend to choose Botnets consisting of multiple bots as this increases the performance of the attack and reduces the likelihood of the Botnet being stopped. The growth in size of Botnets is greatly influenced by the ability of their creators to find and exploit vulnerable systems on the Internet.

Some previous research has discussed how Botnet works in carrying out its actions, which consist of the spread of Botnet on IoT devices involves several stages, namely, first the bot or malware code performs scanning and investigation to find vulnerable IoT devices. Malware code performs scanning and investigation to find vulnerable IoT devices. After locating it, the infection process begins through brute force or vulnerability exploitation methods next, a compatible ver-si of the malware is installed and executed on the device. Once the rent-an IoT device is successfully compromised, it transforms into a bot and starts communicating with the botmaster. In this stage, the bot can recruit new devices and multiply to expand the IoT Botnet network as quickly as possible. During this

phase, the bot maintains a connection with the botmaster and waits for commands. Eventually, after connecting with the botmaster, these bots receive attack orders and execute malicious activities such as DDoS attacks and spam delivery. These stages create an organized pattern of attacks and reflect the complexity of the strategies used by cybercriminals in leveraging IoT devices for malicious activities [26] [27].

In the research conducted by Giachoudis et al. [36] proposed the use of an alightweight agent, which is a software entity installed in each IoT installation to monitor network traffic from IoT devices. These agents work together to collect information about network traffic and detect ongoing DDoS or bot attacks and act as monitoring entities that communicate to protect IoT installations from attacks.

In the research conducted by Wei et al. [34] developed an efficient Network Intrusion Detection System (NIDS) for deployment on IoT devices. This NIDS is capable of detecting Botnet activity at an early stage by using accessible features of IoT network traffic, then implementing a two-stage framework consisting of simple models to quickly identify potentially suspicious traffic, followed using Convolutional Neural Network (CNN) models to detect Botnet activity based on its categories. Convolutional Neural Network (CNN) model to detect Botnet activity based on its categories. This research also proposes a novel scheme to convert IoT traffic into a three-channel Red, Green, Blue (RGB) image which is done by taking the size or data length of the traffic packets sent or received by the IoT device as a feature and grouping them into three different color channels, namely red, green, and blue, each channel representing the packet length information of the inbound, outbound, or combined traffic. This allows the use of image processing methods to handle malicious encrypted traffic. The implementation carried out in this research can improve the security of IoT devices by efficiently and effectively detecting Botnets on IoT in edge computing.

The research conducted by Hasan et al. [30] developed a Hybrid Deep Learning approach by implementing Long-Short-Term Memory (LSTM) and Deep Neural Network (DNN) to Secure the Industrial Internet of Things (IIoT) from botnet attacks. The proposed mechanism is able to identify multi-variant botnet attacks with 99.94% accuracy and is able to cope with increasingly sophisticated botnet attacks. This approach can help improve the security of IIoT infrastructure and prevent botnet attacks that can damage the system.

4.2. System Resources Consumption Attacks

System Resources Consumption Attacks are a type of attack that exploits system resources, such as memory, file system storage, and CPU. These attacks can result in resource exhaustion, cause denial of service that consumes all available resources, and prevent access by legitimate users. These attacks can result in IoT devices becoming slow or even unresponsive, interfering with necessary data processing and forcing devices to spend a lot of energy on inappropriate tasks.

The impact of such attacks is a decrease in overall system availability and performance, potentially leading to decreased device functionality or even complete system failure. The effects are particularly pronounced on targeted IoT devices, where increased use of network and computing resources can lead to overload. Consequently, device performance slows down, and resources such as battery power can be depleted faster than usual. In addition to disrupting the operation of IoT devices in an edge computing environment, such attacks can also incur additional costs, especially if the devices are connected via a paid network. Such attacks can hinder real-time response, which is crucial in IoT infrastructures. [38].

Managing resource consumption efficiently is key to preventing threats to data security and IoT operations and ensuring system availability and responsiveness. With a good understanding of the potential attacks that can disrupt resource consumption, proactive measures in attack mitigation and resource management can be an effective strategy in maintaining the reliability of IoT systems in edge computing [11]. DDoS attacks are a type of sustained attack that aims to hinder or weaken the accessibility of an organization’s resources or services [39]. DDoS and Trojan attacks are often used simultaneously to cause disruption to systems and services. To protect systems from DDoS and other attacks an organization must implement proactive security measures such as continuity improve-

ment, risk evaluation, and the use of security systems. The following are the types of attacks that disrupt System Resources Consumption on IoT edge computing infrastructure.

A. DDoS SYN

During the TCP connection process in the server-client model, the server must receive a Synchronize (SYN) packet from the client. In this process, the server consumes some resources for TCP connection establishment and sends back SYN-ACK packets to the client. Due to the limited resources of the server, if the client does not send an acknowledgment (ACK) packet and many SYN packets from other malicious clients are sent, the server resources may be overloaded, so that the server cannot connect to the client. [39].

In research conducted by Evmorfos et al [40] focuses on techniques for detecting SYN flood attacks that are common in internet-connected devices, such as IoT devices and gateways using the Recurrent Neural Network method with Deep Learning and Long Short-Term Memory (LSTM) Neural Network. In this study, researchers initially explored the use of Recurrent Neural Network (RNN) with Deep Learning by training the model with normal traffic that does not involve attacks to recognize normal traffic patterns so that this model can detect abnormal network traffic that may indicate an attack. Furthermore, it uses the LSTM neural network to detect SYN flood attacks. Overall, this paper provides insight into how to detect SYN attacks on IoT devices and gateways connected to the Internet. The use of RNN and LSTM methods in the context of deep learning provides solutions to security challenges in the edge computing environment, particularly SYN flood attacks on IoT devices.

Then research conducted by Antony et al. [41] used the bash-iptables implementation method to overcome SYN flood attacks on IoT. The method successfully reduced SYN flood attacks by 55.37% and reduced ping flood attacks by 60%. In addition, the paper mentions that the use of the Rule Based Signature Analysis method can help in recognizing SYN flood DDoS attack patterns on IoT. This method recognizes attack patterns by looking for unique attributes in attack packets, so that it can distinguish between traffic that indicates an attack and normal traffic. Thus, the implementation of bash-iptables and rule-based signature analysis methods are two methods that can be used to overcome SYN flood attacks on IoT networks

B. DDoS DNS

Serangan is an exploit where an attacker takes advantage of vulnerabilities in the Domain Name System (DNS) to disrupt the functionality of DNS servers or redirect users to fake websites, as well as intercept or intercept traffic. In the context of IoT in edge computing, DNS attacks can be used to perform malicious activities such as DNS tunneling, disrupting and even severing normally functioning connections within a network, gaining remote access to targeted servers, crippling servers, stealing data, disabling servers, and stealing data, redirecting users to fake sites, and performing DDoS attacks. [42].

Research conducted by Xu et al. [43] explored the use of DNS behavior pattern analysis to develop a DNS traffic monitoring system that can observe and model the behavior of IoT systems in edge networks. Using the DNS temporal-spatial analysis approach, this research successfully identified the communication patterns between IoT systems, cloud servers, and IoT users. They also analyzed the convergence of DNS behavior of various IoT systems. This research utilizes a simple yet effective Bloom filter mechanism in detecting unusual DNS traffic patterns. The use of Bloom filters can help tackle DNS DDoS attacks efficiently due to its ability to quickly process and filter DNS requests, identify and block domain addresses involved in the attack, and reduce the load on the DNS infrastructure by minimizing processing time. The results of this study provide important insights into the DNS request pattern characteristics of heterogeneous IoT systems. This research also explores the application of DNS traffic pattern analysis for security monitoring and anomaly detection, utilizing Bloom filter data structures.

C. Trojan

Trojan is one of the attacks on IoT security that includes attacks on Radio Frequency Identification (RFID) labels of communication networks and on data privacy. [44] acting like the Trojan horse in Greek mythology, Trojans enter the system without the user's knowledge, and once installed, they can perform a variety of malicious

activities such as stealing personal information, deleting or corrupting files, and granting unauthorized access. It is important to maintain security by using the latest security software and adopting wise internet security practices to avoid potential threats from Trojans and other malware attacks.

In the research conducted by Suryono et al. [44] discussed aspects of hardware network security related to Trojans in IoT using literature review. The results of the study state that the security level of IoT devices cannot be fully guaranteed without a solid hardware security foundation. The research emphasizes the need to strengthen the security aspects of hardware to protect IoT devices from Trojan threats. Trojans in hardware can create significant security gaps and can exploit system weaknesses. In addition, this research states the importance of using Side Channel Analysis as an additional layer of security. This approach aims to protect cryptographic keys used to ensure the integrity, confidentiality, and authentication of systems and data on IoT devices. Overall, they state that in order to improve the security of IoT devices, special attention needs to be paid to the hardware security aspect, with additional security layers such as Side-Channel Analysis to protect data and implement cryptographic functions.

In the research conducted by Guo et al. [45] discusses a threat called Hardware Trojan (HT) to IoT security. HT refers to malicious modifications to an Integrated Circuit (IC), which can change the function of the chip or cause sensitive information leakage once activated. In the context of the rapid development of IoT, the security aspect has become very important and HT detection has become a significant research focus. In the study, chip temporal thermal information and Self-Organizing Map (SOM) neural network were used to detect and isolate Trojan-infected chips. Chip temporal thermal information is used to obtain temperature information on the chip, while the SOM neural network is used to classify the chips into two groups, namely the group with Trojan and the group without Trojan. This method proved to be very effective in detecting Trojans on chips. Experiments conducted show that this method is very effective and can detect HT and identify the position of the Trojan with high accuracy.

D. Brute Force

Brute force is an approach in computing where the system tries all possible solutions sequentially and without utilizing the intelligence of the algorithm. In the context of computer security, brute force is often used to break passwords, encryption, or other protection mechanisms by testing all possible combinations until finding the correct one. Brute Force algorithms are used as a technique to match words or strings in text with patterns, by matching each character from left to right [37].

Research conducted by Idris et al. [47] p roposed an approach using time-responsive statistical relationships to detect and visualize Brute Force Attack (BFA) attacks on File Transfer Protocol (FTP) servers in IoT networks. The goal of this research is to provide insight into the types of BFA attacks and generate attack patterns that can assist IoT system administrators in analyzing similar attacks. The method includes extracting important features from data packets related to potential attacks, detecting BFA on FTP services in IoT networks and reflecting an understanding of how FTP attack characteristics may vary over time to visualize FTP attack patterns. Although this research successfully visualizes attack patterns identifying their configurations and provides a clear picture of brute force attack traffic, it does not propose specific methods to prevent BFA attacks, it only focuses on the detection and understanding of attack patterns rather than the implementation of direct prevention solutions.

4.3. Threats to Service Availability

Threats to service availability on IoT in edge computing include attacks that can quickly consume resources, limit bandwidth, and inhibit instant response to services that require real-time conditions, such as security systems [48]. In addition, threats can come from attacks that exploit security vulnerabilities on IoT devices in edge computing, which can result in performance degradation or service failure. These threats can cause an increase in unauthorized traffic, resulting in low service availability or even complete failure. The impact can eliminate the system’s ability to operate optimally, which can disrupt business functions that rely heavily on the continued operation of IoT devices in edge computing environments [49]. In the worst-case scenario, the targeted system could go down completely, causing serious disruption to the services provided and a significant financial impact on the business involved.

The implementation of security measures, such as network traffic monitoring, firewalls, regular system updates, redundancy and backup, is crucial to mitigate the impact of these threats and ensure the availability of IoT services in an edge computing environment. High awareness of potential threats and rapid response are also important in maintaining the smooth operation of such services [18].

In the context of IoT in edge computing, service availability is critical to maintain fast response and reliable operation. Threats to Service Availability include attacks such as worms, viruses, DoS denial-of-service attacks and other malicious activities that are common on the Internet [50]. The following are the types of attacks that disrupt Service Availability on IoT edge computing infrastructure.

A. APTs

APTs are a threat that has attracted widespread attention because they are persistent and difficult to detect. APTs are characterized as prolonged, strategic, and targeted. Prolonged means that these attacks are not limited to a short attack but rather take place over a long period of time, sometimes months or years. This continuity allows the attackers to execute their steps carefully and without the target's knowledge. Additionally, these attacks are more strategic in nature as they involve careful planning. Attackers don't just launch attacks randomly but instead, they carefully plan their every move, select specific targets, and conduct in-depth analysis of the target's system's weaknesses. APTs do not attack just any target, but rather focus on specific organizations, institutions, or individuals. APTs aim to access or collect confidential information from governments, military organizations, or business entities [50]. APTs can affect the security of IoT systems by performing attacks by entering the network and gaining unauthorized access but going undetected for a long period of time. APT attacks can lead to data theft, system destruction, or use of the system for further attacks [51].

In research conducted by Rahman et al [52] made a significant contribution by proposing a framework that combines Artificial Intelligence (AI), blockchain, and Machine Learning at the IoT edge to protect IoT data in Industry 4.0. Experimental results show that the proposed model has superior performance, with data integrity maintained and system efficiency improved. Thus, this method can be considered a positive step in addressing APT threats and improving security in the industry 4.0 ecosystem.

Research conducted by Li et al. [53] examines the use of intelligent systems in detecting persistent and sophisticated threats, namely APTs. Within the scope of edge IoT, this research explores approaches that involve pre-processing and Machine Learning algorithms to detect and classify APTs, with the aim of improving IoT security. In this research, edge IoT is used to improve the responsiveness and speed of detection against APT threats in IoT. The approach used includes pre-processing techniques that include data preparation steps before going into the analysis process. Furthermore, machine learning algorithms are used to detect and classify APTs.

B. Ransomware

Ransomware is a type of malicious software, also known as malware, that encrypts users' files or locks their computers and then demands a ransom to restore access. [54]. It is a form of cyberattack that has become increasingly common in recent years. Ransomware can be spread through phishing emails, malicious websites, or by exploiting software vulnerabilities. Once a system is infected, the ransomware will usually display a message requesting payment in a cryptocurrency such as Bitcoin, in exchange for a decryption key or to unlock the computer. Paying the ransom does not guarantee that files will be recovered, and experts generally advise against doing so. Instead, it is recommended to back up important files regularly and keep software up to date to protect against ransomware attacks.

Research conducted by Al-Hawawreh et al. [55] aims to design an efficient ransomware detection model specifically for secure Industrial Internet of Things (IIoT) systems. IIoT systems are known to be attractive targets for ransomware attacks because they run critical services that affect people's lives and have significant operational costs. human life and have significant operational costs. This research presents a model for ransomware detection model that relies on asynchronous and Peer-to-Peer (P2P) communication between edge gateways connected in an IIoT network. The model utilizes a hybrid feature engineering technique that combines classical and variational

auto-encoder features. This approach enables the development of a ransomware detection model that is more efficient and effective in identifying and preventing ransomware attacks on IoT systems. The uniqueness of this model lies not only in its efficiency, but also in the maintenance of user privacy. By using asynchronous and P2P communication between the edge gateways, this model is designed to maintain the privacy of user data. Thus, this research contributes to the development of security solutions for IIoT that are more robust and reliable, especially in the face of increasingly sophisticated ransomware attacks.

4.4. Threats to Communication

Threats to communication in the context of IoT at edge computing can have a serious impact, as systems depend on communication between IoT devices and data processing centers at the edge [19]. Threats such as cyberattacks, network disruptions, or device failures can disrupt the flow of data, resulting in the loss of critical data, loss of integrity, and hinder the system's ability to make decisions and respond automatically. decisions and respond automatically. This can threaten the reliability, security, and efficiency of IoT operations in edge computing, and potentially cause financial and reputational harm to organizations that rely on these technologies. Good communication quality enables IoT devices to function optimally, maximizing the benefits of IoT technology and making a positive contribution to overall system performance and security. performance and security of the overall system. Good communication quality enables IoT devices to function optimally so as to maximize the benefits of IoT technology and make a positive contribution to overall system performance and security. [56]. Security measures, such as data encryption, traffic monitoring, and protection against DDoS attacks, are crucial to protect vital communication between IoT devices and edge computing infrastructure. This is done while considering the physical security of IoT devices to prevent manipulation or theft. The following are the types of attacks that can disrupt communications on IoT edge computing infrastructure.

A. Sniffing

Eavesdropping is also known as sniffing or snooping. Sniffing is an attack that involves intercepting packets transmitted over a network. Radio-frequency Identification (RFID) devices are vulnerable to this attack, where an attacker can steal critical information such as node identification and configuration. Sniffing attacks on RFID threaten the confidentiality and integrity of data, especially when sensitive information is involved. To protect RFID systems, security measures such as data encryption and the use of secure communication protocols are required to prevent unauthorized access and maintain information security [57]. Sniffing in the context of IoT in edge computing refers to the unauthorized capture of data packets from IoT devices or sensors in edge computing. This can pose a security risk as sensitive information may be exposed to attackers.

In the research conducted by Nie et al. [58] using the CSE-CIC-IDS2018 dataset which is a dataset that contains network traffic data for the identification of cybersecurity attacks and threats, including DDoS attacks and CIC-DDoS2019 is a type of dataset specifically focused on DDoS attacks, and contains relevant data for analyzing and detecting DDoS attacks.

This research aims to identify suspicious patterns of behavior associated with sniffing and other attacks. Once these patterns are identified, appropriate preventive measures can be taken, such as blocking unauthorized access or taking corrective actions to protect sensitive data from such attacks. In addition, this research also plans to combine Convolutional Neural Network (CNN) with Generative Adversarial Network (GAN) method for spatial-temporal feature extraction from network data to assist in attack prevention by identifying suspicious patterns more effectively.

In the research conducted by Shen et al. [59], it emphasizes the importance of implementation of robust security architecture and intrusion detection mechanisms to protect IoT devices and data from packet sniffing attacks in edge computing. Packet sniffing attacks can result in the theft of sensitive information and undermine the security of IoT systems. Therefore, machine learning integration with cryptography in edge computing can help in monitoring and detecting abnormal behavior, thereby preventing packet sniffing attacks and protecting the overall security of IoT systems.

Table 1: List of surveyed papers

Ref.	Network Bandwith Consumption Attack				System Resources Consumption Attacks				Threats to Service Availability		Threats to Communication	
	UDP Flood	ICMP Flood	Worm	Botnet	DDoS SYN	DDoS DNS	Trojan	Brute Force	APTs	Ransom-ware	Sniffing	MiTM
[26]	✓											
[27]	✓											
[30]		✓										
[28]		✓										
[33]			✓									
[36]				✓								
[34]				✓								
[30]				✓								
[40]					✓							
[41]					✓							
[43]						✓						
[44]							✓					
[45]							✓					
[47]								✓				
[52]									✓			
[53]									✓			
[55]										✓		
[58]											✓	
[59]											✓	
[62]												✓

B. Man in The Middle (MiTM)

Man-in-the-Middle (MiTM) attacks pose a significant security risk to IoT in edge computing, as they allow attackers to intercept, monitor, and potentially alter communications between devices or users. [60]. In the context of IoT, MiTM attacks can lead to data breaches, financial losses, and damage to a company's reputation. [61].

In the IoT industry, MITM attacks pose a considerable risk, especially when Supervisory Control and Data Acquisition (SCADA) systems are used to control industrial IoT devices. Therefore, it is important to secure IoT systems by implementing appropriate security policies and using appropriate IoT technologies and protocols.

In the research conducted by Fereidouni et al. [62] There is a discussion of various methods of countering MitM attacks, although the specifics of the methods are not outlined. Some common methods that can be used to mitigate MitM attacks include DNS spoofing, Secure Socket Layer (SSL) stripping, and Address Resolution Protocol (ARP) spoofing. In addition, this paper also discusses some potential solutions to prevent and mitigate MitM attacks on IoT networks, focusing on data encryption, strong authentication, network traffic monitoring, network segmentation, and regular software updates.

Table 1 provides a summary list of the papers discussed in section IV. Table 1 is classified by cybersecurity attacks and threats based on what aspects can affect the infrastructure, services and communications in IoT edge computing. Among them are attacks that can consume network bandwidth capacity, consume system resources, disrupt service availability that can hinder the normal functioning of services and can disrupt the communication process in a network or system.

5. Analysis and Discussion

In analyzing and discussing the results of our survey, some interesting findings require further evaluation. It was found that several patterns of cyberattacks emerged consistently across literature, providing an overview of the main risks in the IoT paradigm in edge computing. However, along with the solutions presented in several studies, several security aspects have not received in-depth attention, creating potential gaps that need to be addressed immediately. In this discussion, we will provide an opinion on these trends, highlight the success of mitigation strategies used in the literature, and detail areas that may need improvement. This approach will not only provide an evaluation of the survey results but also provide a foundation for a better understanding of the direction cybersecurity research is taking in the context of IoT in edge computing.

In this discussion, we will present our opinion on the efficacy of the mitigation strategies described in the literature, as well as detail areas that may need improvement. This approach not only provides an evaluation of the survey results but also provides a basis for a better understanding of the direction cybersecurity research is taking in the context of IoT in edge computing.

Threats and attacks on IoT in edge computing, especially through the exploitation of security weaknesses in IoT devices and infrastructure, are classified into four categories: na, network bandwidth consumption attacks, system resource consumption attacks, threats to service availability, and threats to communication. Each attack and threat have its own characteristic, so it also requires a different solution. After conducting a survey, the results of the solution or method that can be implemented in each type of attack or threat that occurs in IoT in edge computing were obtained.

In the context of the solutions and methods documented in Table 2 related to various attacks on IoT infrastructure in edge computing. As seen in the table, the solutions provided cover both preventive and response measures to specific security threats. Further analysis highlights the importance of addressing these three aspects to strengthen the security of IoT infrastructure.

Overcoming Network Bandwith Consumption Attacks is by setting Access Control, namely setting strict rules to control who can access the IoT network, using software or hardware to filter and monitor data traffic to detect attacks that try to flood the network with many requests so that if there is abnormal activity in network traffic, the system will quickly deal with the attack such as using a firewall and detection and prevention system with Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) can also help detect and prevent suspicious or dangerous traffic. Based on a survey conducted, one of the most influential and dangerous attacks that affects network bandwidth consumption is because it utilizes a large network of infected devices, which allows attackers to launch large-scale DDoS attacks. This attack generates a very high volume of network traffic from different sources, making it difficult to identify and mitigate. Unlike UDP or ICMP flood attacks that come from limited sources, botnet attacks are more complex and difficult to handle.

Overcoming System Resource Consumption Attacks is done by conducting continuous System Health Monitoring. Continuous System Health Monitoring is conducting periodic checks to check the health of the system and notify if there is an abnormal spike in resource usage and conducting access control and isolation by limiting access to IoT devices and system resources to authorized parties only. With this monitoring, attacks can be detected immediately, and actions can be taken to reduce their impact, such as redirecting workloads or limiting resources for suspicious entities. Based on a survey conducted, one of the most influential and dangerous attacks in consuming system resources is a trojan because of its ability to operate silently and consume limited system resources. Unlike direct attacks such as DDoS, Trojans infiltrate IoT devices by disguising themselves as legitimate software, making them difficult to detect. Once inside the system, Trojans slow down device operations, damage, steal sensitive data, or install other malware.

In addressing Threats to Service Availability in IoT in edge computing, the focus is on redundancy and efficient monitoring. Redundancy means having a backup system ready to take over if the primary system fails, minimizing service downtime. Regular monitoring allows for the early detection of problems so they can be

Table 2: Solution based on attack type

Classification Dimensions	**Types of Attacks**	**Solution / Method**
Network Bandwith Consuption Attack	UDP Flood	Leverage Edge functions as a reverse proxy and ShadowNet to protect against UDP flood attacks with responsive detection based on real-time statistics.
		IDS based on J48 algorithm on UDP flood attacks serves to detect suspicious traffic patterns, enabling rapid response and attack mitigation to protect the network.
	ICMP Flood	Packet Filtering Firewall and Circuit Level Gateway Firewall are used in ICMP flood attacks to filter and control suspicious ICMP traffic and prevent network overload.
		FlowGuard in ICMP flood attacks is used to detect and prevent intrusions by monitoring suspicious ICMP traffic patterns.
	Worm	Diversity software in worms is used to increase security by changing software components, such as versions or configurations, thereby inhibiting the worm's ability to spread and damage hosts with uniform weaknesses.
	Botnet	Lightweight Agents in botnets are used to infiltrate target systems efficiently, playing a role in remote control by attackers without causing excessive impact on the performance of the attacked system.
		The IoT traffic conversion scheme into three-channel RGB images is used in conjunction with NIDS to improve botnet attack detection by leveraging image processing techniques to identify suspicious patterns or behaviors in IoT devices.
System Resource Consumption Attack	DDoS SYN	RNN with Deep Learning and LSTM to detect SYN flood attacks on IoT devices and gateways connected to the internet, involving training the model using normal traffic to recognize typical traffic patterns.
		Bash-iptables is by implementing iptables firewall rules with Bash scripts to block or mitigate suspicious traffic that can be indicated as SYN flood attacks, thereby protecting the system from overloading and maintaining service availability.
	DDoS DNS	DNS temporal-spatial analysis and bloom filtering are used to detect and filter suspicious DNS traffic, separating legitimate requests from potential DDoS attacks to protect DNS infrastructure from overload.
	Trojan	Side-Channel Analysis is used to collect secret information from a target system through side or indirect channels, such as power consumption or response time, without easily detectable traces.
		Chip Temporal Thermal Information and Self-Organizing Map (SOM) which can detect or trick security systems by analyzing temperature changes on the chip and using unsupervised learning algorithms to map trojan activity patterns.
	Brute Force	Using time-responsive statistical relationships to detect and visualize Brute Force Attacks
Threats to Service Availability	APTs	Building a framework that combines Artificial Intelligence, Blockchain, and Machine Learning at the IoT edge to enhance IoT data security in Industry 4.0, successfully maintaining data integrity and improving system efficiency against APT threats.
		Exploring approaches involving pre-processing and machine learning algorithms.
	Ransomware	Relies on asynchronous and P2P communication between edge gateways connected in an IoT network.
Threats to Communication	Sniffing	Combining CNN with GAN methods for spatial-temporal feature extraction from network data.
		The integration of machine learning with cryptography in edge computing in sniffing aims to improve anomaly detection, encrypt data, provide real-time monitoring, recognize attack patterns, and optimize system performance to protect data integrity and communication security.
	MiTM	DNS spoofing, SSL stripping, and ARP spoofing are used to redirect, break SSL encryption, and manipulate communication between two parties in order to gain control over the information sent and received.

addressed immediately. In addition, it is important to keep the system up to date with the latest security updates

and ensure that the system can adjust its capacity when there is a surge in demand to prevent overload. The overall strategy keeps the service running without interruption, even when facing problems or attacks. Based on a survey conducted, Ransomware is considered one of the most dangerous threats that disrupt service availability, hindering the normal functioning of services because of its fast and immediate destructive ability. Ransomware can quickly lock important information and require victims to pay a sum of money to obtain the decryption key. The impact is not only in the loss of access to data but also because these attacks often ask for large ransoms, creating financial pressure on victims and even damaging the company's reputation. Therefore, although APTs may be more difficult to detect in the long term, the immediate threat and pressure posed by Ransomware make it one of the most impactful and disruptive attacks in cybersecurity today that can hinder the normal functioning of services.

In addressing Threats to Services Communication on IoT in edge computing, we focus on strengthening communication security and identity validation. The use of encryption in data exchange between IoT devices is essential to ensure that data sent and received are difficult to intercept or manipulate by unauthorized parties. According to a survey conducted, MiTM attacks are attacks that have a major impact on the communication process in a network or system. In the context of edge computing, where data processing is carried out closer to IoT devices to optimize performance, MiTM attacks can be a serious threat to communication security. MiTM creates opportunities for attackers to infiltrate between communicating IoT devices, opening the potential for data manipulation or even stopping the flow of information so that this attack can cause serious and detrimental service disruptions. IoT devices in edge computing environments often use wireless connections.

By implementing these security measures, communication within the IoT network in edge computing becomes more protected from external attacks and threats. The introduction of multiple solutions to prevent such attacks aims to minimize their occurrence, enhance system resilience, and ensure smooth operations and service reliability in edge computing environments. These proactive measures not only safeguard data integrity and device functionality but also bolster confidence in the overall IoT infrastructure, creating a foundation for robust and secure operations.

To further strengthen the security and reliability of edge computing, mitigation strategies must be prioritized to anticipate and minimize the impact of cyberattacks that could disrupt the performance of IoT devices. Mitigation involves the implementation of monitoring systems to detect potential threats early, the application of preventive measures to fortify system defenses, and the management of rapid, efficient responses to ensure that any attacks do not compromise the overall performance of devices and networks [63]. These steps, when combined with proactive security measures, form a comprehensive approach to maintaining the security and stability of edge computing systems.

5.1. Intrusion Detection System (IDS)

IDS is a security system that plays a role in monitoring and monitoring network activity to detect threats or cyber attacks, IDS will help network administrators make decisions faster to prevent cyber attacks such as DDoS attacks from spreading faster so that they can disrupt system performance [64]. The main purpose of IDS is to protect system security based on three main aspects of information security, namely Confidentiality helps maintain data confidentiality by ensuring that only authorized parties can access certain information [65], such as when someone tries to access confidential data without authorization, the IDS will detect this activity and provide a warning, Integrity is the IDS ensures that data is not altered, tampered with, or manipulated by unauthorized parties [66], If a hacker tries to change data in the system without authorization, the IDS will log this activity and report it to the administrator and availability plays a role in ensuring that systems and data are always accessible to legitimate users without interruption due to cyberattacks.

There are several types of IDS, namely Host Based Detection (HIDS) which analyzes the behavior of specific computer systems to detect attacks and Network Based Detection (NIDS) analyzes network traffic to identify malicious activity. Host-Based Intrusion Detection System (HIDS) works by detecting threats or attacks by analyzing changes to system files, user activity logs, as well as running processes. If there is suspicious activity, such as unauthorized file changes, unauthorized access, or malicious programs running in the background, the HIDS will alert the network administrator. There are two main methods used in HIDS, namely rule-based detection and

Table 3: Difference between HIDS and NIDS

Aspects	**HIDS**	**NIDS**
Monitoring Location	Installed on devices such as computers, servers and operating systems.	Installed inside a network firewall or router.
Object Analyzed	System logs, file changes, user activity, running processes.	Network traffic.
Threat Types Detected	Malware, unauthorized file changes, suspicious activity in the system.	Network-based attacks such as DDoS, sniffing, and illegal access.
Response to Threats	Provides alerts and can take automatic actions in the system.	Sends alerts to administrators and can be combined with an Intrusion Prevention System (IPS).
Detection Coverage	Limited only to the device on which the HIDS is installed.	Covers the entire network and connected devices.

Table 4: Difference between reguler firewall and NGFW

Aspects	**Regular Firewall**	**NGFW**
Traffic Monitoring	Filtering by IP address, port, and protocol (Layer 3 and 4).	Has deeper monitoring, including content inspection and deep packet inspection (DPI).
Application inspection (the ability to inspect and recognize applications in network traffic)	Can’t recognize specific apps	Can recognize apps in more detail, even if some are hidden.
Security Integration	Working separately and independently, firewalls only function to block or allow network traffic based on predefined rules, without connecting or collaborating with other security systems.	Integrates with other security systems. This means that, in addition to filtering network traffic, NGFW can cooperate with detection systems (IDS/IPS), which detect and prevent further threats or attacks. In addition, NGFW can also connect with web application protection (WAF).

anomaly-based detection [67]. Network Based Detection (NIDS), which works by monitoring and analyzing data traffic passing through a network to detect suspicious activity or cyberattacks.NIDS are usually placed at key points in the network, such as behind a firewall or gateway, so that it can monitor the communication that occurs between devices within the network as well as connections from outside [68].

Both types of IDS have advantages and disadvantages, Table 3 compares NIDS and HIDS from various aspects to provide a comprehensive overview of the types of IDS that can be implemented based on security cases.

5.2. Next-Generation Firewall (NGFW)

Next-Generation Firewall (NGFW) is a modern firewall designed to protect networks from increasingly sophisticated cyber attacks. Unlike traditional firewalls that only filter traffic based on IP addresses and ports, NGFW has broader capabilities, such as deep inspection of the contents of data packets (DPI) and Intrusion Prevention System (IPS). With these features, NGFW can detect, and block threats hidden in network traffic, including malware attacks, application exploits, and suspicious encrypted communications and can also decrypt SSL/TLS traffic to check if there are attacks hiding in encrypted communications. With the integration of cloud security and IoT device protection [69], [70].

Other advantages are application-based control capabilities and user identity, where NGFW can recognize applications used in the network and restrict access based on defined security policies and is also easier to manage than traditional firewalls because it has a dashboard-based interface and supports security for cloud infrastructure and IoT devices, so as to protect cloud-based services and edge computing from exploitation [71], Thus, NGFWs can be a more effective security solution in facing the challenges of modern cyberattacks than traditional firewalls.

5.3. Sysmon (System Monitor) in Edge Computing

Sysmon is a system activity monitoring tool integrated in the Windows operating system and can be downloaded to monitor the information log in the Windows event log. By using Sysmon, the information obtained becomes more detailed and clearer, as this tool provides in-depth additional data for analysis, such as information about internet connections, process behavior, and file changes. Therefore, if there is any suspicious activity, Sysmon will log it, so that the data can be used for security analysis and responding to potential threats [72]. To view Sysmon logs on a Windows system using Event Viewer, open the navigation pane on the left and select Applications and Services Logs. Then, find the folder named Microsoft-Windows-Sysmon/Operational and click on it to access the logs that Sysmon has logged [73].

Sysmon can provide highly detailed logs of various system activities, such as executed processes, network connections, changes to files, and more. In the context of edge computing, where many devices operate autonomously in dispersed locations, this in-depth monitoring is critical. It enables early detection of problems or potential threats, before they spread or affect the larger system [74].

5.4. Artificial Intelligence, Deep Learning & Machine Learning for Cyber Attack Detection

Machine Learning (ML) and Artificial Intelligence (AI) play a crucial role in improving cybersecurity by automatically detecting, preventing and responding to threats. ML can analyze patterns in data and identify anomalies that indicate cyberattacks, while AI can classify threats and provide appropriate responses [75].

One of the important roles of DL and ML is in the authentication and authorization process of IoT devices. Since these devices are widespread in various networks and are often not equipped with good security features, DL and ML can be used to verify legitimate devices by recognizing the normality patterns of these devices [76]. Machine learning models can be trained to detect devices with normal behavior and flag suspicious activity, so that unauthorized devices can be instantly blocked before they can access the network.

In addition, DL and ML are also effective in detecting anomalies or unusual activities in IoT networks. With continuous learning capabilities, these models are able to recognize normal patterns of network behavior and detect any activity that deviates from those patterns, such as illegal access attempts, suspicious spikes in data traffic, or unusual device interactions. This capability enables rapid mitigation of potential attacks such as botnets, DDoS, or man in the middle attacks, which often target vulnerable IoT devices [77].

DL and ML also enable the implementation of prediction-based security systems. Predictive models trained with historical data can provide early warnings before an attack occurs. For example, DL tools can predict the likelihood of zero-day attacks or ransomware attacks on IoT devices based on detected anomaly patterns. With this predictive capability, security systems can take early preventive action and significantly reduce the impact of an attack [78].

In addition, automation of the incident response process is a big advantage of DL and ML integration in IoT device security. Once a threat is detected, the system can respond automatically, for example by disconnecting the infected device or restricting access to certain networks. This reduces reliance on manual human effort, thereby speeding up the response process and minimizing potential damage [79], [80]. Implementing these four points provides a clear picture of how edge devices can be protected from various cyber threats with simple yet effective steps. Table 5 provides clarity on the security role sections discussed and provides real application examples for easy understanding.

6. Conclusion

This paper comprehensively addresses the security challenges and mitigations arising from the integration of IoT in edge computing. Security is not only related to the risk of attacks and threats but also affected by limited resources and close interconnection between devices in the edge computing environment. In the face of these challenges, security risk mitigation is an important aspect that cannot be ignored by configuring and implementing data encryption as proactive measures. This mitigation effort is not only a response to risk, but also a strategy that

Table 5: The role of mitigation implementation in maintaining edge computing security

Safety Aspects	Role in security
Detection of strange behavior outside of normal patterns	Monitor device activity. If there is any abnormal behavior, such as sudden transmission of large data, the system will provide an alert.
Authentication and Authorization	The system checks the devices that want to connect to the network. If the device is not recognized or is suspicious, access will be blocked.
Automated Response to Attacks	If a threat is found, the system takes immediate action such as disconnecting the device or restricting access.
Attack Prediction Ability	The system learns from previous attack patterns to forecast possible future attacks and prevent them early.

can significantly reduce the chances of attacks and threats in the implementation of IoT in edge computing. Attacks and threats that affect Network Bandwidth Consumption, System Resource Consumption, Threats to Service Availability, and Threats to Communication are the focus points in formulating the taxonomy in this research.

The results of this survey highlight the importance of security in Internet of Things (IoT) implementations in edge computing. While some mitigation strategies have been identified, the findings indicate that some aspects of security still require more in-depth attention, creating potential gaps that need to be addressed immediately. A focus on configuration control and the implementation of data encryption as proactive measures are key in addressing security risks. are key in addressing security risks. These measures are not only a response to risks, but also a significant strategy to reduce the chances of attacks and threats on IoT implementations in edge computing. By applying relevant solutions to attacks and threats affecting infrastructure, services, and communications, it is expected that communications in IoT networks in edge computing environments can become more protected, maintain data integrity, and improve the overall operational smoothness of the system.

It is hoped that the survey paper written can provide in-depth knowledge and understanding of the security risks and threats associated with the topic of IoT in edge computing, provide insights into solutions to these challenges and is able to provide an overview of further research and development in the field of IoT in edge computing.

CRediT Authorship Contribution Statement

Tiara R. Hadiningrum: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Data Curation, Writing – Original Draft, Visualization, Funding Acquisition. **Resky A. D. Talasari:** Validation, Formal analysis, Resources, Writing – Review & Editing. **Karina F. Ilham:** Validation, Investigation, Data Curation, Writing – Review & Editing. **Royyana M. Ijtihadie:** Conceptualization, Methodology, Writing – Review & Editing, Supervision, Project Administration, Funding Acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declaration of Generative AI and AI-assisted Technologies in The Writing Process

The authors used generative AI to improve the writing clarity of this paper. They reviewed and edited the AI-assisted content and take full responsibility for the final publication.

References

[1] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol. 73, no. 1, pp. 3–25, Jul. 2019, doi: 10.1007/s11235-019-00599-z.

[2] M. I. Hussain, "Internet of Things: challenges and research opportunities," *CSI Transactions on ICT*, vol. 5, no. 1, pp. 87–95, Dec. 2016, doi: 10.1007/s40012-016-0136-6.

[3] A. Al-Ali, R. Gupta, I. Zualkernan, and S. K. Das, "Role of IoT technologies in big data management systems: A review and Smart Grid case study," *Pervasive and Mobile Computing*, vol. 100, p. 101905, May 2024, doi: 10.1016/j.pmcj.2024.101905.
[4] O. K. Sulaiman and A. Widarma, "SISTEM INTERNET OF THINGS (IOT) BERBASIS CLOUD COMPUTING DALAM CAMPUS AREA NETWORK," Sep. 2017, doi: 10.31227/osf.io/b6m79.
[5] X. Jin, C. Katsis, F. Sang, J. Sun, A. Kundu, and R. Kompella, "Edge Security: Challenges and Issues." [Online]. Available: https://arxiv.org/abs/2206.07164
[6] A. Adhitama and T. Informasi, "Keamanan Edge Computing untuk Perangkat IoT Tersebar."
[7] S. Javanmardi, A. Nascita, A. Pescapè, G. Merlino, and M. Scarpa, "An integration perspective of security, privacy, and resource efficiency in IoT-Fog networks: A comprehensive survey," *Computer Networks*, vol. 270, p. 111470, Oct. 2025, doi: 10.1016/j.comnet.2025.111470.
[8] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021, doi: 10.1109/jiot.2020.3015432.
[9] M. Taimoor Khan, "Towards Practical and Formal Security Risk Analysis of IoT (Internet of Things) Applications," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, Sep. 2022, pp. 1–4. doi: 10.1109/etfa52439.2022.9921511.
[10] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0268-2.
[11] S. Millar, "IoT Security Challenges and Mitigations: An Introduction." [Online]. Available: https://arxiv.org/abs/2112.14618
[12] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/j.dcan.2019.08.006.
[13] E. Fazeldehkordi and T.-M. Grønli, "A Survey of Security Architectures for Edge Computing-Based IoT," *IoT*, vol. 3, no. 3, pp. 332–365, Jun. 2022, doi: 10.3390/iot3030019.
[14] H. Kalariya, K. Shah, and V. Patel, "An SLR on Edge Computing Security and possible threat protection." [Online]. Available: https://arxiv.org/abs/2212.04563
[15] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019, doi: 10.1109/jproc.2019.2918437.
[16] P. P. Ray, D. Dash, and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," *Journal of Network and Computer Applications*, vol. 140, pp. 1–22, Aug. 2019, doi: 10.1016/j.jnca.2019.05.005.
[17] R. Smith, D. Palin, P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "Battery draining attacks against edge computing nodes in IoT networks," *Cyber-Physical Systems*, vol. 6, no. 2, pp. 96–116, Jan. 2020, doi: 10.1080/23335777.2020.1716268.
[18] R. Ghadiri and M. Elhajj, "Security and Performance Analysis of Edge Computing in IoT," in *2023 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, IEEE, Nov. 2023, pp. 542–548. doi: 10.1109/comnetsat59769.2023.10420709.
[19] W. Najib, S. Sulistyo, and Widyawan, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 9, no. 4, pp. 375–384, Dec. 2020, doi: 10.22146/jnteti.v9i4.539.
[20] R. Jansen, T. Vaidya, and M. Sherr, "Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor," in *28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1823–1840. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/jansen
[21] A. Kumar and D. Singh, "Detection of Security Attacks on Edge Computing of IoT Devices through NS2 Simulation," *Journal of Physics: Conference Series*, vol. 2327, no. 1, p. 12016, Aug. 2022, doi: 10.1088/1742-6596/2327/1/012016.
[22] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS Attack & its Effect in Cloud Environment," *Procedia Computer Science*, vol. 49, pp. 202–210, 2015, doi: 10.1016/j.procs.2015.04.245.
[23] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," *International Journal of Safety and Security Engineering*, vol. 12, no. 5, pp. 577–588, Nov. 2022, doi: 10.18280/ijsse.120505.
[24] S.-H. Lee, Y.-L. Shiue, C.-H. Cheng, Y.-H. Li, and Y.-F. Huang, "Detection and Prevention of DDoS Attacks on the IoT," *Applied Sciences*, vol. 12, no. 23, p. 12407, Dec. 2022, doi: 10.3390/app122312407.
[25] E. Gelenbe and M. Nasereddin, "Protecting IoT Servers Against Flood Attacks with the Quasi Deterministic Transmission Policy," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, Nov. 2023, pp. 379–386. doi: 10.1109/trustcom60117.2023.00068.
[26] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards IoT-DDoS Prevention Using Edge Computing," in *USENIX Workshop on Hot Topics in Edge Computing (HotEdge 18)*, Boston, MA: USENIX Association, Jul. 2018. [Online]. Available: https://www.usenix.org/conference/hotedge18/presentation/bhardwaj
[27] H. Nihri, E. S. Pramukantoro, and P. H. Trisnawan, "Pengembangan IDS Berbasis J48 Untuk Mendeteksi Serangan DoS Pada Perangkat Middleware IoT," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 12, pp. 6902–6907, 2018, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3795
[28] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9552–9562, Oct. 2020, doi: 10.1109/jiot.2020.2993782.
[29] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities," *IEEE Access*, vol. 8, pp. 205340–205373, 2020, doi: 10.1109/access.2020.3037108.
[30] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," *International Journal of Safety and Security Engineering*, vol. 12, no. 5, pp. 577–588, Nov. 2022, doi: 10.18280/ijsse.120505.
[31] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Future Generation Computer Systems*, vol. 89, pp. 525–538, Dec. 2018, doi: 10.1016/j.future.2018.06.053.
[32] S. Hilt, F. Mercês, M. Rosario, and D. Sancho, "Worm war: The botnet battle for IoT territory," *URL: https://documents. trendmicro. com/assets/white_papers/wpworm-war-the-botnet-battle-for-iot-territory. pdf.(Accessed 3 October 2022)*, 2020.
[33] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: A software diversity approach," *Ad Hoc Networks*, vol. 47, pp. 26–40, Sep. 2016, doi: 10.1016/j.adhoc.2016.04.011.
[34] C. Wei, G. Xie, and Z. Diao, "A lightweight deep learning framework for botnet detecting at the IoT edge," *Computers & Security*, vol. 129, p. 103195, Jun. 2023, doi: 10.1016/j.cose.2023.103195.

[35] P. Beltrán-García, E. Aguirre-Anaya, P. J. Escamilla-Ambrosio, and R. Acosta-Bermejo, "IoT Botnets," in *Telematics and Computing*, Springer International Publishing, 2019, pp. 247–257. doi: 10.1007/978-3-030-33229-7_21.

[36] N. Giachoudis, G.-P. Damiris, G. Theodoridis, and G. Spathoulas, "Collaborative Agent-based Detection of DDoS IoT Botnets," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, IEEE, May 2019, pp. 205–211. doi: 10.1109/dcoss.2019.00055.

[37] T. Hasan *et al.*, "Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2952–2963, Sep. 2023, doi: 10.1109/tnse.2022.3168533.

[38] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," in *2017 1st Cyber Security in Networking Conference (CSNet)*, IEEE, Oct. 2017, pp. 1–3. doi: 10.1109/csnet.2017.8242006.

[39] L. Huraj, M. Šimon, and T. Horák, "Resistance of IoT Sensors against DDoS Attack in Smart Home Environment," *Sensors*, vol. 20, no. 18, p. 5298, Sep. 2020, doi: 10.3390/s20185298.

[40] S. Evmorfos, G. Vlachodimitropoulos, N. Bakalos, and E. Gelenbe, "Neural network architectures for the detection of SYN flood attacks in IoT systems," in *Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments*, in PETRA '20. ACM, Jun. 2020, pp. 1–4. doi: 10.1145/3389189.3398000.

[41] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, pp. 43–52, Nov. 2021, doi: 10.30812/matrik.v21i1.1078.

[42] O. S. M. B. H. Almazrouei, P. Magalingam, M. K. Hasan, and M. Shanmugam, "A Review on Attack Graph Analysis for IoT Vulnerability Assessment: Challenges, Open Issues, and Future Directions," *IEEE Access*, vol. 11, pp. 44350–44376, 2023, doi: 10.1109/access.2023.3272053.

[43] K. Xu, F. Wang, S. Jimenez, A. Lamontagne, J. Cummings, and M. Hoikka, "Characterizing DNS Behaviors of Internet of Things in Edge Networks," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7991–7998, Sep. 2020, doi: 10.1109/jiot.2020.2999327.

[44] D. Suryono, "Analisis Keamanan Jaringan Hardware Trojan Pada IoT," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 4, pp. 3529–3537, Dec. 2022, doi: 10.35957/jatisi.v9i4.2845.

[45] S. Guo, J. Wang, Z. Chen, Y. Li, and Z. Lu, "Securing IoT Space via Hardware Trojan Detection," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11115–11122, Nov. 2020, doi: 10.1109/jiot.2020.2994627.

[46] X. Liu, R. Zhou, S. Shimizu, R. Chong, Q. Zhou, and X. Zhou, "Novel MITM attack scheme based on built-in negotiation for blockchain-based digital twins," *Digital Communications and Networks*, vol. 11, no. 1, pp. 256–267, Feb. 2025, doi: 10.1016/j.dcan.2023.11.011.

[47] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating Brute Force Attack Patterns in IoT Network," *Journal of Electrical and Computer Engineering*, vol. 2019, pp. 1–13, Apr. 2019, doi: 10.1155/2019/4568368.

[48] P. Radanliev *et al.*, "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, Jun. 2020, doi: 10.1186/s42400-020-00052-8.

[49] M. Ficco, D. Granata, M. Rak, and G. Salzillo, "Threat Modeling of Edge-Based IoT Applications," in *Quality of Information and Communications Technology*, Springer International Publishing, 2021, pp. 282–296. doi: 10.1007/978-3-030-85347-1_21.

[50] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating Brute Force Attack Patterns in IoT Network," *Journal of Electrical and Computer Engineering*, vol. 2019, pp. 1–13, Apr. 2019, doi: 10.1155/2019/4568368.

[51] X. Cheng, J. Zhang, and B. Chen, "Cyber Situation Comprehension for IoT Systems based on APT Alerts and Logs Correlation," *Sensors*, vol. 19, no. 18, p. 4045, Sep. 2019, doi: 10.3390/s19184045.

[52] Z. Rahman, X. Yi, and I. Khalil, "Blockchain-Based AI-Enabled Industry 4.0 CPS Protection Against Advanced Persistent Threat," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6769–6778, Apr. 2023, doi: 10.1109/jiot.2022.3147186.

[53] Z. Li, X. Cheng, J. Zhang, and B. Chen, "Predicting Advanced Persistent Threats for IoT Systems Based on Federated Learning," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, Springer International Publishing, 2021, pp. 76–89. doi: 10.1007/978-3-030-68851-6_5.

[54] T. A. Ahanger, U. Tariq, F. Dahan, S. A. Chaudhry, and Y. Malik, "Securing IoT Devices Running PureOS from Ransomware Attacks: Leveraging Hybrid Machine Learning Techniques," *Mathematics*, vol. 11, no. 11, p. 2481, May 2023, doi: 10.3390/math11112481.

[55] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "Asynchronous Peer-to-Peer Federated Capability-Based Targeted Ransomware Detection Model for Industrial IoT," *IEEE Access*, vol. 9, pp. 148738–148755, 2021, doi: 10.1109/access.2021.3124634.

[56] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-Computing Architectures for Internet of Things Applications: A Survey," *Sensors*, vol. 20, no. 22, p. 6441, Nov. 2020, doi: 10.3390/s20226441.

[57] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2018. doi: 10.1109/ccnc.2018.8319297.

[58] L. Nie *et al.*, "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 134–145, Feb. 2022, doi: 10.1109/tcss.2021.3063538.

[59] T. Shen, L. Ding, J. Sun, C. Jing, F. Guo, and C. Wu, "Edge Computing for IoT Security: Integrating Machine Learning with Key Agreement," in *2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, IEEE, Jan. 2023, pp. 474–483. doi: 10.1109/iccece58074.2023.10135211.

[60] C. Simko, "Man-in-the-Middle Attacks." [Online]. Available: https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/

[61] "How to Combat MITM Attacks in Edge Environments." [Online]. Available: https://edgelabs.ai/blog/how-to-combat-mitm-attacks-in-edge-environments/

[62] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," *SECURITY AND PRIVACY*, vol. 8, no. 2, Mar. 2025, doi: 10.1002/spy2.70016.

[63] A. Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices," in *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, IEEE, Jul. 2017, pp. 1631–1636. doi: 10.1109/cyber.2017.8446380.

[64] M. Agoramoorthy, A. Ali, D. Sujatha, M. R. T. F, and G. Ramesh, "An Analysis of Signature-Based Components in Hybrid Intrusion Detection Systems," in *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, IEEE, Dec. 2023, pp. 1–5. doi: 10.1109/iccebs58601.2023.10449209.

[65] K. Timraz, T. Barhoom, and T. Fatayer, "A Confidentiality Scheme for Storing Encrypted Data through Cloud," in *2019 IEEE 7th Palestinian International Conference on Electrical and Computer Engineering (PICECE)*, IEEE, Mar. 2019, pp. 1–5. doi: 10.1109/picece.2019.8747193.

[66] C. Sasikala and C. S. Bindu, "A study on remote data integrity checking techniques in cloud," in *2017 International Conference on Public Key Infrastructure and its Applications (PKIA)*, IEEE, Nov. 2017, pp. 43–48. doi: 10.1109/pkia.2017.8278959.

[67] F. Rehman, F. Mushtaq, and H. Zaman, “A Host-based Intrusion Detection: Using Signature-based and AI-driven Anomaly Detection for Enhanced Cybersecurity*,” in *2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, IEEE, Oct. 2024, pp. 1–7. doi: 10.1109/icodt262145.2024.10740248.

[68] L. A. H. Ahmed, Y. A. M. Hamad, and A. A. M. A. Abdalla, “Network-based Intrusion Detection Datasets: A Survey,” in *2022 International Arab Conference on Information Technology (ACIT)*, IEEE, Nov. 2022, pp. 1–7. doi: 10.1109/acit57182.2022.9994201.

[69] B. Singh and S. S. Cheema, “Next Generation Firewall and Self Authentication for Network Security,” in *2023 Seventh International Conference on Image Information Processing (ICIIP)*, IEEE, Nov. 2023, pp. 707–713. doi: 10.1109/iciip61524.2023.10537758.

[70] T. Sarkorn and K. Chimmanee, “Review on Zero Trust Architecture Apply In Enterprise Next Generation Firewall,” in *2024 8th International Conference on Information Technology (InCIT)*, IEEE, Nov. 2024, pp. 255–260. doi: 10.1109/incit63192.2024.10810611.

[71] K. Neupane, R. Haddad, and L. Chen, “Next Generation Firewall for Network Security: A Survey,” in *SoutheastCon 2018*, IEEE, Apr. 2018. doi: 10.1109/secon.2018.8478973.

[72] M. Okuma, K. Watarai, S. Okada, and T. Mitsunaga, “Automated Mapping Method for Sysmon Logs to ATT&CK Techniques by Leveraging Atomic Red Team,” in *2023 6th International Conference on Signal Processing and Information Security (ICSPIS)*, IEEE, Nov. 2023, pp. 104–109. doi: 10.1109/icspis60075.2023.10343783.

[73] R.-V. Mahmoud, M. Anagnostopoulos, S. Pastrana, and J. M. Pedersen, “Redefining Malware Sandboxing: Enhancing Analysis Through Sysmon and ELK Integration,” *IEEE Access*, vol. 12, pp. 68624–68636, 2024, doi: 10.1109/access.2024.3400167.

[74] C. Grimshaw, B. Lachine, T. Perkins, and E. Coote, “Link-based Anomaly Detection with Sysmon and Graph Neural Networks,” in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2024, pp. 1–6. doi: 10.1109/icaic60265.2024.10433846.

[75] D. Puthal, S. P. Mohanty, A. K. Mishra, C. Y. Yeun, and E. Damiani, “Revolutionizing Cyber Security: Exploring the Synergy of Machine Learning and Logical Reasoning for Cyber Threats and Mitigation,” in *2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/isvlsi59464.2023.10238483.

[76] S. Kumar, B. P. Singh, and V. Kumar, “A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security,” in *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, IEEE, Dec. 2021, pp. 1963–1967. doi: 10.1109/icac3n53548.2021.9725596.

[77] T. M. Ghazal, M. K. Hasan, R. A. Zitar, N. A. Al-Dmour, W. T. Al-Sit, and S. Islam, “Cybers Security Analysis and Measurement Tools Using Machine Learning Approach,” in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, IEEE, May 2022, pp. 1–4. doi: 10.1109/icaic53980.2022.9897045.

[78] Z. T. Pritee, M. H. Anik, S. B. Alam, J. R. Jim, M. M. Kabir, and M. Mridha, “Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review,” *Computers & Security*, vol. 140, p. 103747, May 2024, doi: 10.1016/j.cose.2024.103747.

[79] A. Punia, M. Tiwari, and S. S. Verma, “A machine learning-based efficient anomaly detection system for enhanced security in compromised and maligned IoT Networks,” *Results in Engineering*, vol. 26, p. 105562, Jun. 2025, doi: 10.1016/j.rineng.2025.105562.

[80] Arti, K. P. Dubey, and S. Agrawal, “An Opinion Mining for Indian Premier League Using Machine Learning Techniques,” in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, IEEE, Apr. 2019, pp. 1–4. doi: 10.1109/iot-siu.2019.8777472.