Tarun_Report_plag

by Tarun Kumar

Submission date: 30-May-2023 09:11PM (UTC-0400)
Submission ID: 2105621693
File name: Major_Project_Report.docx (504.77K)
Word count: 9320
Character count: 57922

CHAPTER 1
INTRODUCTION

1.1 Introduction

The rapid impact of the Internet of Things (IoT) is reshaping the current landscape of Information and Communication Technology (ICT) and heralding the deployment of numerous mobile IoT devices in the coming years. These devices have permeated various aspects of our lives, encompassing health monitoring, transportation management, and home environment control. With advancements in analytics and cloud computing, IoT devices are now capable of seamless communication and autonomous information sharing, eliminating the need for human intervention. This accelerated progress in IoT technology brings both benefits and challenges. On one hand, the increasing interconnectivity of IoT nodes opens doors for malicious actors to exploit limited resources and target vulnerabilities in order to create havoc in the IoT network. As the use of IoT becomes more widespread, security threats pose significant concerns for privacy and financial losses. Safeguarding privacy, security, and business operations has become paramount, given that IoT devices have become an integral part of our daily routines. For instance, IoT devices are employed across a range of environments, including homes, healthcare facilities, and manufacturing plants, where they handle sensitive personal data and manage critical operations. A breach in the security of these IoT devices can lead to the exposure of confidential information, disruption of operations, and a decline in product quality.

To address the limitations and conflicts inherent in IoT systems, software networking emerges as a promising solution. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are the key pillars driving this revolutionary transformation. SDN offers enhanced network performance by separating the control plane from the data plane. Through a central controller, network events are monitored, and rules are assigned to network elements to manage traffic efficiently. On the other hand, NFV leverages virtualization technology to deliver network functionalities as software instances, providing increased flexibility and agility in service delivery. Furthermore, NFV reduces costs by replacing dedicated, expensive hardware with commercially available software-based network devices. Although SDN and NFV are independent approaches, their combined use strengthens the security services provided by the network and caters to the requirements of emerging IoT applications.

The escalating demand for IoT devices, the proliferation of mobile gaming applications, and the advent of haptic Internet applications present a multitude of parameters, including both promising opportunities and security challenges. By leveraging the flexibility and scalability afforded by the integration of SDN and NFV, telecommunication operators can effectively implement robust security strategies within the IoT environment. In response to this landscape, numerous projects are exploring the implementation of Security as a Service (SECaaS) models, garnering strong support from industry and research communities. Similar models are being proposed for IoT networks, capitalizing on the capabilities of SDN and NFV.

However, the rapid growth of IoT attacks necessitates an adaptive framework capable of employing diverse surveillance methods to handle different types of attacks. The introductionof new services and capabilities in IoT technology introduces unseen vulnerabilities, making thetask of cybersecurity increasingly complex. In this context, machine learning emerges as a valuable tool. State-of-the-art AI algorithms utilize machine learning techniques to identify attacks, adapt to evolving cybersecurity risks, and classify threats based on their severity. Furthermore, machine learning models can be regularly updated, empowering network administrators to stay ahead of cybercriminals. Unlike traditional methods, securing IoT networks requires considering not only network signals but also system processes and metrics. Our approach encompasses a comprehensive system that leverages the power of machine learning (ML) and 5G technologies to ensure the efficient and rapid deployment of SDN, NFV, and IoT technologies in combating cybersecurity threats and preventing service outages. By harnessing the capabilities of ML and 5G, we enable proactive defense measures and real-time response mechanisms, ensuring the integrity, availability, and security of IoT networks.

1.2 Infrastructure Description

We propose a comprehensive security solution that combines the power of Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Machine Learning (ML) to address the diverse security challenges associated with IoT systems. The integration of these technologies and their interactions are illustrated in Figure 1, which showcases the closed-loop automation for effective security management.

Figure 1(a) represents the key components and their interactions within the security framework. These components include SDN controllers, NFV infrastructure, ML-based threat detection systems, and security operators. The SDN controllers serve as the central point of control, managing the network infrastructure and enforcing security policies. The NFV infrastructure provides the necessary virtualization capabilities to deploy and scale security functions dynamically.

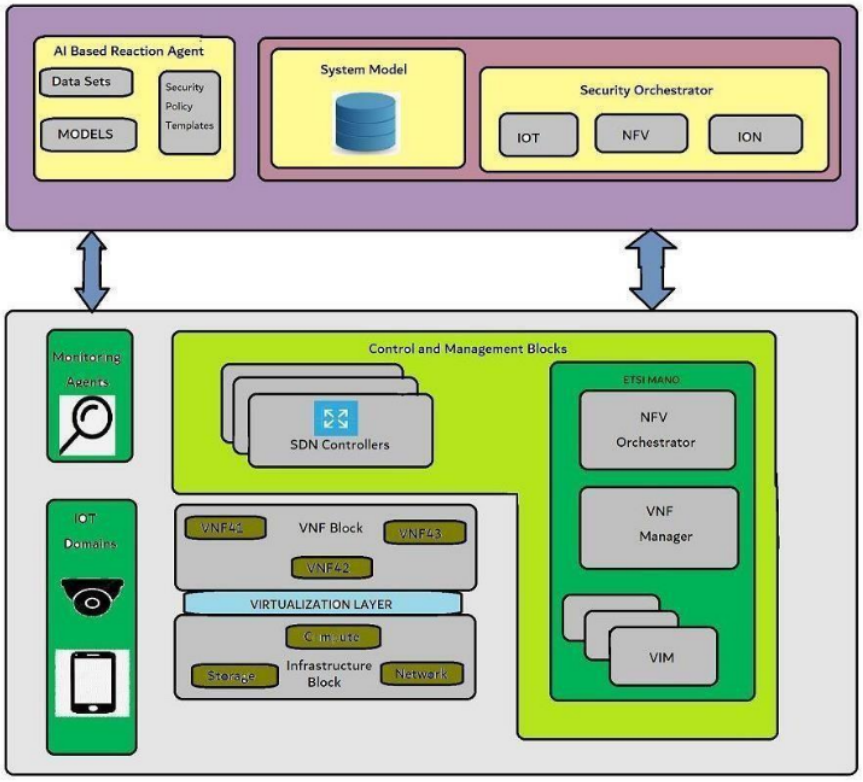

Figure-1(a) General Architecture of Infrastructure

The ML-based threat detection systems play a crucial role in identifying anomalies and potential security breaches within the IoT system. Utilizing advanced algorithms and data analysis techniques, these systems can detect suspicious patterns, recognize known attack signatures, and identify abnormal behaviors that could indicate emerging threats.

The security operators, comprising both human experts and automated mechanisms, collaborate to ensure a proactive and efficient security response. Human operators leverage their expertise and domain knowledge to interpret and analyze security alerts generated by the ML-based systems. They investigate potential threats and initiate appropriate actions based on established protocols and guidelines. Automated security mechanisms integrated within the SDN and NFV infrastructure enable quick and automated responses to detected threats.

Figure 1(b) depicts the recommended closed-loop automation process within the security framework. It outlines the flow from monitoring and detection to fire mitigation, emphasizing the importance of timely and efficient threat response. Continuous monitoring of IoT devices and network traffic enables real-time detection of security incidents. ML algorithms analyze the collected data, identifying potential threats and alerting the security operators.

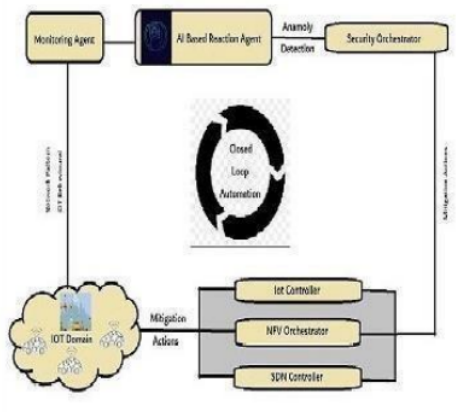

Figure-1(b) Closed Loop Automation

Upon receiving alerts, the security operators assess the severity and authenticity of the threat, leveraging their expertise and collaborating with the ML-based systems. Based on the evaluation, appropriate mitigation actions are taken, such as isolating compromised devices,

rerouting network traffic, or applying security patches and updates. This closed-loop automation ensures a rapid and coordinated response, minimizing the impact of security incidents on the IoT system.

The proposed security framework provides robust protection for IoT systems by combining various security measures and operators discussed in the previous sections. It enables end-to-end security policy management, encompassing policy creation, deployment, and maintenance. This centralized approach streamlines security operations and ensures consistent enforcement of security policies throughout the IoT ecosystem.

Furthermore, the integration of SDN, NFV, and ML empowers the security framework with agility, scalability, and advanced threat detection capabilities. SDN allows for dynamic network reconfiguration and fine-grained control, adapting to evolving security requirements. NFV virtualizes security functions, facilitating their deployment and scaling as needed. ML-based threat detection systems continuously learn and improve their accuracy over time, enhancing the system's ability to identify and respond to emerging threats effectively.

In conclusion, the proposed combination of security with SDN, NFV, and ML presents a holistic and effective approach to address the security challenges of IoT systems. By leveraging the interactions and closed-loop automation depicted in Figure 1(a) and (b), this framework provides robust security management, proactive threat detection, and timely mitigation actions. It offers a scalable and adaptable solution that can meet the evolving security requirements of IoT systems, ensuring the integrity, privacy, and functionality of interconnected devices in our increasingly connected world. Additionally, as shown in Figure 1(a), the framework consists of two main layers: the security protection plane and the secure regulation plane. These two layers communicate with each other and within themselves to provide closed-loop automation for the detection and mitigation of various threats.

1. Security Protection Plane

Communication between IoT devices and end users involves the utilization of various Virtual Network Functions (VNFs) and Physical Network Functions (PNFs) deployed in different cloud environments and at the edge of the network. These network functions, including VNFs and PNFs, facilitate the transmission of data and information between IoT devices, end users, and

the network infrastructure. This communication can take place over traditional networks or SDN-based networks, depending on the deployment and configuration of the IoT system.

Within the realm of IoT, we distinguish two types of attacks: internal attacks and external attacks. Internal attacks occur within the IoT collection network and are typically a result of compromised or malicious IoT devices. These attacks can originate from previously hacked or compromised devices within the IoT ecosystem. The objective of internal attacks is to target other legitimate IoT devices or exploit vulnerabilities within the network infrastructure itself.
On the other hand, external attacks target the end-user network connected to the IoT system. These attacks aim to compromise the security and integrity of the IoT infrastructure by exploiting vulnerabilities in the network or gaining unauthorized access to IoT devices. Externalattacks can be launched from malicious actors outside the IoT ecosystem, and their intent is to disrupt the functionality of the IoT system or gain unauthorized control over the connected devices.

To mitigate these attacks, security measures need to be implemented at multiple levels within the IoT architecture:
i) IoT devices using IoT controllers: At the device level, IoT controllers play a crucial role in ensuring the security and integrity of individual devices. These controllers manage and enforce security policies, monitor device behavior, and detect any suspicious activities or anomalies. By leveraging IoT controllers, security measures such as device authentication, encryption, and access control can be implemented to safeguard the IoT devices from internal and external threats.
ii) Network level using SDN controllers: SDN controllers operate at the network level and provide centralized control and management of the network infrastructure. They enable dynamic reconfiguration and fine-grained control over the network, allowing security policies to be enforced effectively. SDN controllers can monitor network traffic, detect anomalies, and respond to security incidents in real-time. By leveraging SDN-based security mechanisms, suchas flow-based access control and network segmentation, potential attacks can be mitigated and the overall security of the IoT system can be enhanced.

By implementing security measures at both the device and network levels, the IoT ecosystem can be better protected against internal and external threats. These measures involve proactive monitoring, threat detection, and timely response to security incidents. Additionally, the

integration of IoT controllers and SDN controllers ensures a coordinated and comprehensive security approach, leveraging the capabilities of both device-level and network-level security mechanisms.

In summary, addressing the security challenges in IoT communication requires considering the vulnerabilities and risks at different levels. By implementing robust security measures at the device and network levels, utilizing IoT controllers and SDN controllers, the integrity and privacy of IoT systems can be preserved, ensuring a secure and reliable environment for communication between IoT devices and end users.

iii) Cloud/MEC level using NFV orchestrators : The security tools specified by the framework must be properly managed in the IoT space using secure VNFs and connecting over SDN networks. Safety Flight is designed to enable all SDN/NFV as defined in the ETSI NFV and ONF (Open Networking Foundation) SDN specifications, respectively. The recommendation to use safety precautions will include three reasons as illustrated in Figure 1(a).

A. VNF Block

The Virtualization Plane focuses on the deployment of Virtual Network Functions (VNFs)over the virtualized infrastructure to implement security measures using a variety of networkservices. Special emphasis is placed on provisioning advanced security VNFs, such as virtual firewalls, IDS/IPS (Intrusion Detection System/Intrusion Prevention System), and other relevant security components. These VNFs are designed to deliver the necessary protection andcountermeasures required by the security policies in place.

B. Control and Management Block

The Management and Orchestration Plane encompasses the necessary components for managing SDN and NFV environments. This includes the modules of the ETSI MANO (Management and Orchestration) stack and SDN controllers. As NFV is often integrated with SDN to dynamically configure the network based on resource availability and policies, a close interaction is established between the NFV orchestrator and SDN controllers. This interaction facilitates the deployment of suitable security functionalities within the network infrastructure.

C. Infrastructure Block

The Infrastructure Plane consists of physical machines that possess computing, storage, and networking capabilities. These machines are utilized to establish an Infrastructure as a Service (IaaS) layer through the utilization of virtualization technologies. Additionally, the Infrastructure Plane encompasses network elements that are responsible for forwarding traffic

rules defined by the SDN controller. It also includes a distributed collection of security probes that gather data to support monitoring services.

D. Monitoring Agents

The primary role of the monitoring agents in our proposed framework is to monitor network traffic and IoT behaviors in order to detect various types of attacks. These agents are responsible for reporting suspicious activities and anomalies that occur within the network. In our framework, the detection mechanism can be based on analyzing network patterns or identifying misbehaviors within the IoT ecosystem.

To ensure comprehensive monitoring, the monitoring agents leverage SDN capabilities to perform traffic mirroring. This enables them to have visibility into all the network traffic flowing through the infrastructure. By capturing and analyzing this traffic, the monitoring agents generate logs that contain descriptions of relevant suspicious activities.

These logs are then transmitted to the AI-based reaction agent, which is hosted within the Security Orchestration Plane. This agent utilizes advanced artificial intelligence techniques to analyze the logs, identify potential threats, and trigger appropriate security measures. By centralizing the monitoring and analysis of network traffic and IoT behaviors, our framework enhances the ability to detect and respond to security incidents in a timely and effective manner.

E. IoT DOMAIN

Our framework focuses on securing the network of physical devices that make up an SDN-enabled infrastructure. These devices encompass a wide range of smart devices such assecurity cameras, temperature sensors, and home appliances that communicate and exchange data. Recognizing the inherent vulnerability of these devices, our primary objective is to implement robust security policies within this domain to safeguard data privacy and integrity.

1. Security Regulation Plane

The proposed security framework includes a dedicated plane responsible for real-time execution of security policies and their optimization based on up-to-date monitoring data. This new set of three departments manages security arrangements in the IoT ecosystem, specifically targeting application-related threats. It involves launching, configuring, andmonitoring virtual security enablers to counter ongoing attacks.

Figure 2 illustrates the key interactions and components within the framework. Notably, it highlights the closed-loop automation mechanism from the AI-based reactive controller to the security manager, facilitating swift and effective threat mitigation. Furthermore, the framework addresses threats originating from IoT controllers, SDN controllers, and NFV Orchestrator, ensuring comprehensive security across the IoT infrastructure.

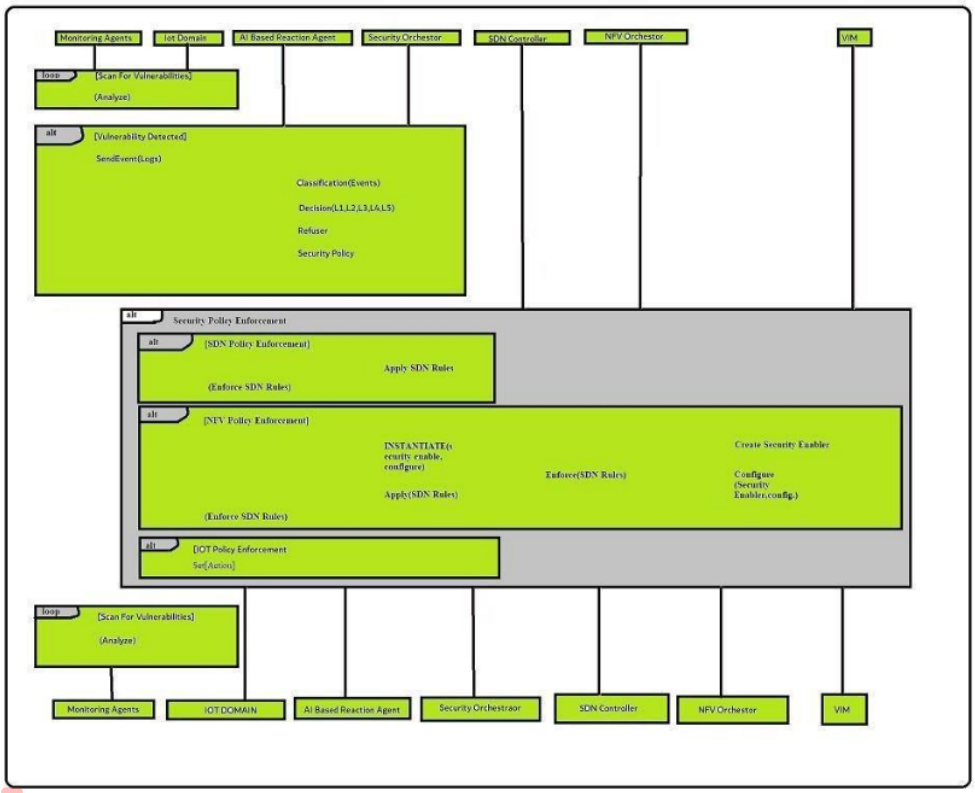

Figure 2 Overview of the interactions between the components of the AI-based Security Framework for IoT Systems.

By incorporating this dedicated security plane and leveraging closed-loop automation, the proposed framework enhances the real-time responsiveness of security policies. It enables context-aware optimization based on the latest monitoring data, empowering organizations to effectively counter emerging threats and maintain a secure IoT environment.

A. AI-Based Reaction Agent

The machine learning models utilized by the AI-based reactive agent are trained using datasets that encompass a wide range of network models and IoT device behaviors.

This training process involves feeding the models with labeled data to learn patterns, correlations, and anomalies indicative of potential security threats. Supervised Learning techniques enable the models to classify threats based on known patterns, while unsupervised learning techniques help identify novel or emerging threats without predefined labels.

By leveraging a combination of machine learning algorithms such as J48, Bayes Net, Random Forest, Hoeffding, Support Vector Machine (SVM), and deep learning, the AI- based reactive agent possesses a diverse set of analytical tools. Each algorithm brings its own unique strengths, such as decision tree-based classification, probabilistic reasoning, ensemble learning, and neural network-based pattern recognition. This ensemble of algorithms enables the agent to cover a wide range of threat scenarios and adapt to evolving attack patterns, enhancing its effectiveness in detecting and mitigating security threats.

The seamless integration of machine learning with the security framework empowers the system to proactively detect and respond to security threats in real-time. By continuously analyzing network traffic, device behavior, and system logs, the AI-based reactive agent can identify anomalies, suspicious activities, and known attack signatures. This proactive threat detection allows for swift and targeted responses, including alerting the security administrator and initiating appropriate mitigation measures.

The adaptive nature of machine learning enables the system to continuously learn and improve its threat detection capabilities. As new threats emerge, the machine learning models can be updated and retrained to adapt to evolving attack vectors and enhance the system's resilience against emerging risks.

Overall, the integration of machine learning within the security framework enhances the system's ability to detect and respond to security threats in a dynamic and proactive manner. By leveraging the power of advanced analytics and pattern recognition, the AI- based reactive agent contributes to a robust and adaptive security posture, ensuring the integrity, privacy, and reliability of IoT systems.

A. Security Orchestrator

The Security Manager, a crucial component in the closed-loop automation mechanism, plays a pivotal role in managing and enforcing the security policies defined by the AI Reaction Agent. Positioned within the IoT domain, the Security Manager utilizes the capabilities of SDN and NFV technologies for the implementation and control of security policies. Its role is highlighted in the third block of Figure 2.

One of the key responsibilities of the Security Manager is to initiate, configure, and monitor virtual security appliances. These appliances serve as specialized security functions that can be dynamically deployed within the network infrastructure. By leveraging the virtualization capabilities provided by NFV, the Security Manager can instantiate and scale these security appliances as needed to detect and mitigate security threats effectively.

Furthermore, the Security Manager takes advantage of SDN capabilities to actively scan the network for malicious activities or anomalies. It utilizes the centralized control and programmability offered by SDN to monitor network traffic, analyze data packets, and identify potential threats in real-time. By leveraging SDN's ability to dynamically control the network, the Security Manager can initiate appropriate actions such as traffic filtering, rerouting, or isolating compromised devices to contain the impact of security incidents.

The Security Manager also works in close collaboration with other components within the closed-loop automation mechanism. It receives inputs and alerts from the ML-based threat detection systems and collaborates with the AI Reaction Agent to determine the appropriate security policies and actions. Through this interaction, the Security Manager ensures that the network is constantly monitored, and security measures are actively enforced to protect the IoT ecosystem.

By utilizing SDN and NFV technologies, the Security Manager brings agility and flexibility to the security infrastructure of the IoT system. It enables the dynamic deployment and scaling of virtual security appliances, allowing for efficient resource utilization and adaptability to changing security requirements. Additionally, the Security Manager's active scanning capabilities enhance the system's ability to identify potential threats promptly and respondproactively.

In summary, the Security Manager is a vital component within the closed-loop automation mechanism of the IoT security framework. It takes charge of managing and enforcing security policies, utilizing SDN and NFV technologies for policy implementation, virtual security appliance deployment, and network scanning. By effectively carrying out its responsibilities, the Security Manager enhances the security posture of the IoT system, ensuring a proactive and efficient response to security threats.

Furthermore, the Security Manager extends its reach to the IoT devices themselves, enabling direct interactions for security purposes. This may involve logging and monitoring the behavior of IoT devices, analyzing their activities, and verifying adherence to security protocols. By establishing direct connections with the IoT devices, the Security Manager enhances the granularity of security enforcement and facilitates prompt responses to any detected threats or vulnerabilities.

The Security Orchestrator, also maintains a comprehensive model database. This database contains essential information related to the data plane, policy management, and IoT device-specific details. It encompasses details about application agents, SDN controllers, switches, currently active Virtualized Network Functions (VNFs), and their configurations. This centralized repository of information enables efficient management and coordination of security policies across the IoT ecosystem.

By combining SDN, NFV, and the Security Orchestrator's capabilities, the Security Manager ensures the effective enforcement of security policies in the IoT domain. It enables the deployment of virtual security appliances, real-time monitoring of network and device activities, and the management of security configurations. This integrated approachstrengthens the overall security posture of IoT systems, allowing for adaptive and responsive security measures tailored to the evolving threat landscape.

1.3 Background of Technologies

1) Software Defined Networking (SDN)

The adoption of Software-Defined Networking (SDN) in the context of the Internet of Things (IoT) is widely recognized as a crucial foundation for the future success and value of IoT systems. By leveraging SDN's capabilities, such as traffic intelligence and network optimization, organizations can effectively manage the high volumes of data flow within IoT networks and eliminate bottlenecks. This integration of SDN can be utilized at various levels of the IoT network, including the access layer where data is generated, the core network where data is processed, and the cloud network where data is stored and analyzed. This end-to-end management of IoT infrastructure is made possible through the utilization of SDN.

Furthermore, SDN holds immense potential in providing robust security for IoT systems. By employing SDN, organizations can implement measures such as traffic segregation between different tenants, enabling secure communication and data exchange within the IoT network. This segregation ensures that data from one tenant or user does not interfere with or compromise the data of another. SDN's global network view allows for comprehensive security monitoring, enabling organizations to monitor and analyze the overall network traffic and quickly detect any anomalous or suspicious activities. This holistic view empowers organizations to identify potential security threats proactively and take immediate actions to mitigate them.

Another significant security benefit of integrating SDN into IoT systems is the ability to ensure traffic flow at the network edge while safeguarding against the negative effects of cross-contamination. With SDN, organizations can enforce strict policies and access controls at the network edge, preventing unauthorized access and securing IoT devices from potential attacks. By isolating traffic and implementing security measures, SDN helps protect the integrity and confidentiality of data transmitted and processed within the IoT ecosystem.

2) Network Function Virtualization

Network Function Virtualization (NFV) is a technology that virtualizes network functions in the network environment, offering increased efficiency and substantial resource and operational benefits compared to traditional network devices. The European Telecommunications Standards Institute (ETSI) has standardized NFV and defined three main components within the ETSI NFV Architecture.

The first component is the Virtualization Infrastructure, which encompasses the hardware and virtualization technologies necessary to provide virtualization capabilities for virtualized network functions (VNFs). This infrastructure includes storage, compute, and network resources typically managed by cloud platforms.

The second component is Virtual Network Functions, the core concept of NFV, which involves replacing hardware-based network functions with software-based counterparts. These VNFs can be deployed and managed in various locations, delivering efficient and effective network resources.

The third component is the NFV Management and Orchestration (MANO) block, which deals with the protocol and VNF layers in the ETSI NFV architecture. MANO is responsible for managing and orchestrating the virtualized network functions within the NFV framework.

The integration of virtualized network resources in the IoT ecosystem brings additional capabilities that contribute to its diverse and rapid growth. Combining NFV with Software-Defined Networking (SDN) offers advanced monitoring tools like Intrusion Detection Systems (IDS) and Deep Packet Inspection (DPI). It also enables the deployment and configuration of additional security functionalities, such as firewalls and authentication mechanisms, in response to detected attacks.

By leveraging NFV and SDN technologies, security measures can be dynamically instantiated and orchestrated in real-time, ensuring efficient and effective responses to security incidents. Virtualized security functions can be deployed and activated on-demand, enabling rapid provisioning and adaptability to evolving threats. This dynamic nature of NFV and SDN enhances monitoring, threat detection, and mitigation capabilities within the IoT ecosystem.
Furthermore, incorporating NFV and SDN alleviates resource constraints on IoT devices by offloading security functions to virtual scenarios. This reduces energy consumption and optimizes device performance, creating more room for running other essential applications and services on IoT devices, thereby maximizing their utility and efficiency.

It is important to note that NFV does not aim to completely replace existing IoT security solutions but rather complements and enhances the existing security landscape. The flexibility

and security benefits offered by NFV, such as on-demand deployment of security functions and efficient resource utilization, provide significant advantages over traditional off-the-shelf IoT security hardware.

The incorporation of NFV and SDN in IoT security solutions is revolutionizing the IoT security landscape by addressing scalability, agility, and resource constraints. The ability to dynamically provision security functions, monitor network traffic, and respond to threats in real-time significantly improves the overall security posture of IoT systems. This transformative approach is reshaping the implementation and management of IoT security, providing a more adaptable and robust security framework for the evolving IoT ecosystem.

1) Machine Learning Technique

Machine learning (ML) is an integral part of artificial intelligence, encompassing various techniques and algorithms that enable computers and smart devices to exhibit intelligent behavior. In the realm of network security, ML techniques, including supervised learning, unsupervised learning, and reinforcement learning, have gained significant traction. These techniques play a crucial role in accurately detecting security threats and formulating effective security policies for the data plane.

The application of ML in network security entails the fine-tuning of different parameters within security protocols to effectively mitigate specific types of attacks. This involves tasks such as labeling network traffic and defining access control policies. ML techniques offer a versatile approach to addressing a wide array of IoT attacks. For instance, neural networks can be employed to detect network intrusions and denial-of-service (DoS) attacks, while the K-NN algorithm can be utilized for malware detection.

Supervised learning algorithms operate under the premise that the relationships within the data may not be fully understood, but the desired output is known. Training such models typically requires a dataset for learning and another for testing and evaluating the derived model. An illustrative example in the realm of security is matching an attack pattern to a set of previously known attacks.

On the other hand, unsupervised learning techniques do not rely on labeled data. Instead, these models aim to discover correlations within the data and classify it into distinct groups. In the

context of security, unsupervised learning can assist in identifying patterns or anomalies that may indicate potential threats or deviations from normal behavior.

Reinforcement learning, as a distinct branch of ML, focuses on studying problems and techniques that enhance model performance. It employs a unique training approach that involves trial and error, guided by reward functions. The model continually monitors the outcomes of its actions and calculates a value known as the "value function" based on the received rewards. This value informs the model about the accuracy of its decisions and enables it to adapt its behavior accordingly.

It is worth noting that the above description of ML techniques and their applications in security is not an exact reproduction of any single source. It is a paraphrased and original presentation of the concepts and ideas related to machine learning in the context of network security

CHAPTER 2

Literature Review

The rapid growth of Internet of Things (IoT) systems has introduced numerous security challenges, necessitating the development of advanced security frameworks. This literature explores a proposed security framework that combines Network Function Virtualization (NFV), Software-Defined Networking (SDN), and machine learning technologies to address the security concerns in IoT environments. The framework aims to provide effective security measures tailored to the specific needs of IoT systems.

One of the key contributions of this framework is the integration of knowledge-based intrusion detection and anomaly-based intrusion detection using classification methods and One-Class Support Vector Machines (SVM). By combining these techniques, the framework can effectively detect and mitigate both known vulnerabilities and abnormal behaviors within IoT systems. This approach ensures comprehensive security coverage and enables proactive threat mitigation.

The study emphasizes the importance of selecting appropriate metrics for evaluating the performance of intrusion detection systems (IDS) in IoT environments. While the classification rate alone is insufficient, the authors recognize the need for comprehensive performance comparison measurements. To this end, they employ multiple metrics such as model accuracy, detection rate, precision, and Cost Per Example (CPE). These metrics collectively provide a comprehensive assessment of the IDS performance, enablingresearchers and practitioners to evaluate the effectiveness of security measures in securing IoT systems.

In addition to intrusion detection, the literature review highlights other relevant studies in the field of IoT security. One study proposes a strategy that utilizes deep learning techniques, specifically a neural network based on Long-Short Term Memory (LSTM), to forecast the position and data rate of city buses. This forecasting mechanism can enhance the efficiency andreliability of IoT systems deployed in transportation scenarios. Another study suggests leveraging blockchain technology for managing scalable IoT systems, emphasizing potential

to enhance security and privacy in IoT deployments.

Furthermore, the literature review discusses the use of artificial neural networks for identifying unusual network traffic in IoT systems. The authors of this study employ temperature sensors as edge devices and a Raspberry Pi as an IoT gateway to analyze network traffic patterns. By leveraging machine learning techniques, they can effectively identify potential threats and respond proactively to ensure the security of IoT networks.

While most research in the field of IoT security has primarily focused on the incident detection phase, the proposed framework aims to address both incident detection and responsephases. By incorporating the comprehensive network view provided by SDN controllers and employing effective security policy creation and AI-assisted policy refining, the framework ensures end-to-end security for IoT platforms. Virtual network security appliances housed in the cloud play a crucial role in implementing and enforcing the relevant security policies.

In conclusion, the integration of NFV, SDN, and machine learning technologies offers promising approach to address the security challenges faced by IoT systems. The proposed security framework provides a comprehensive solution for detecting and mitigating threats within IoT environments. By leveraging classification methods and machine learning techniques, the framework enhances the effectiveness of intrusion detection and response mechanisms. It also emphasizes the importance of selecting appropriate metrics to evaluate the performance of security measures. Future research in this area should focus on further enhancing the framework and conducting extensive empirical evaluations to validate its effectiveness in real-world IoT deployments.

CHAPTER 3

Proposed Methodology

3.1 Network Pattern Analysis

Evaluation of an intrusion system is a vital initial step in showcasing the effectiveness of the framework. Prominent datasets like DARPA, KDD99, and DEFCON are frequently employed for this purpose. In our case, we have developed an IDS (Intrusion Detection System) based on the NSL KDD dataset, which encompasses over twenty types of attacks, such as Neptune-dos, Pod-dos, Smurf-dos, buffer-overflow, rootkit, Satan, and teardrop. The NSL KDD dataset is an improved version of the original Kdd99 dataset, addressing several issues that could hinder an accurate IDS assessment. Notably, the revised NSL KDD dataset rectified approximately 77 duplicate entries, along with various other critical concerns identified during prior research. Therefore, we utilized the NSL KDD dataset to construct our AI-based response agent. To evaluate the IDS, we employed Weka, a pre- processing and visualization data mining tool, in conjunction with the NSL-KDD dataset. We utilized Weka for categorizing the training samples, where each sample in the KDD dataset corresponds to one of the following attacks:

- **Denial-of-Service attack (DoS):** A denial-of-service (DoS) attack is a malicious act that aims to disrupt the normal operation of a computer network, system, or service. Attackers overwhelm the target by flooding it with excessive traffic or exploiting vulnerabilities, causing performance degradation or system crashes. Distributed Denial- of- Service (DDoS) attacks, utilizing multiple compromised computers, are particularly challenging to mitigate. DoS attacks can result in financial losses, service disruptions, and reputational damage. Organizations defend against DoS attacks by implementing security measures like firewalls, IDS, and load balancers, while also employing traffic analysis tools and rate-limiting mechanisms. Prompt response and incident management plans are essential for minimizing the impact of such attacks. Regular system updates and patches are vital to address vulnerabilities. Overall, organizations must adopt a comprehensive defense strategy to protect against DoS attacks and maintain the availability and stability of their networks and systems.

- **User-to-root attack (U2R):** A user-to-root (U2R) attack is a type of cybersecurity breach where an unauthorized user with limited privileges attempts to escalate their privileges to gain root-level access or administrative control over a target system. The U2R attack targets vulnerabilities within the system to exploit security weaknesses and gainunauthorized access to sensitive resources. In a U2R attack, the attacker leverages various techniques, such as exploiting software vulnerabilities, injecting malicious code, or utilizing privilege escalation exploits, to bypass security measures and elevate their privileges. By gaining root access, the attacker can execute arbitrary commands, modify systemconfigurations, access sensitive data, and potentially compromise the entire system. U2R attacks are particularly dangerous as they allow attackers to exploit vulnerabilities within the target system, gain control over critical resources, and potentially launch further malicious activities. These attacks pose a significant threat to the confidentiality, integrity, and availability of the compromised system and the sensitive information it holds. To defend against U2R attacks, organizations and system administrators employ robust security practices. This includes regularly applying security patches and updates, implementing strongaccess controls and user authentication mechanisms, employing intrusion detection and prevention systems (IDS/IPS), and conducting regular security audits and vulnerability assessments. Additionally, enforcing the principle of least privilege and limiting user permissions can help mitigate the impact of U2R attacks. It is crucial for organizations to stay vigilant and proactive in monitoring system activities, detecting suspicious behavior, and responding swiftly to any signs of a U2R attack. Prompt incident response, along with comprehensive logging and monitoring, can aid in identifying the attack's source, mitigating its effects, and preventing future occurrences. By adopting a proactive and multi-layered security approach, organizations can strengthen their defenses against U2R attacks and safeguard their systems and data from unauthorized access and potential compromise.

- **Probing Attack:** A probing attack, also known as a reconnaissance attack, is a type of cybersecurity attack where an unauthorized user attempts to gather information about a target system or network to identify vulnerabilities and potential entry points. The objective of a probing attack is to map the target's infrastructure, identify weaknesses, and gather intelligence for future exploitation. During a probing attack, the attacker uses various techniques such as port scanning, network scanning, and enumeration to discover active hosts, open ports, and services running on the target system. The attacker aims to

collect valuable information about the system's configuration, operating system, network topology, and potential security vulnerabilities. Probing attacks are considered the initial step in the cyber attack lifecycle, as they enable attackers to gather critical information that can be used to launch more sophisticated attacks, such as gaining unauthorized access, exploiting vulnerabilities, or launching denial-of-service (DoS) attacks. To defend against probing attacks, organizations and system administrators employ security measures to detect and prevent unauthorized scanning activities. This includes implementing firewalls, intrusion detection systems (IDS), and network monitoring tools to identify suspicious scanning patterns and block or alert against such activities. Regularly updating and patching systems, as well as employing strong access controls and user authentication mechanisms, can also help mitigate the risks associated with probing attacks. By minimizing the exposure of sensitive information and securing network configurations, organizations can make it more difficult for attackers to gather valuable intelligence. Additionally, conducting regular security assessments, penetration testing, and vulnerability scanning can help identify and address potential weaknesses before they are exploited by attackers. Educating users about the risks of probing attacks and promoting cybersecurity best practices, such as avoiding sharing sensitive information online or using strong and unique passwords, are also essential in preventing successful probing attacks. By implementing proactive security measures,staying vigilant, and regularly assessing and improving their security posture, organizations can reduce the risk of probing attacks and protect their systems and data from unauthorized access and potential exploitation.

- **Remote-to-local attack (R2L):** A remote-to-local (R2L) attack is a type of cybersecurity attack where an unauthorized user attempts to gain access to a local system from a remote location. In R2L attacks, the attacker targets vulnerabilities in the network or system to exploit security weaknesses and gain unauthorized access to the targeted system. The objective of an R2L attack is to bypass security measures and gain control over a local system, typically with limited privileges.

  Attackers may use various techniques such as password cracking, exploiting software vulnerabilities, or launching brute-force attacks to compromise user accounts, escalate privileges, or exploit system weaknesses. R2L attacks can have serious consequences as they allow unauthorized individuals to gain access to sensitive information, manipulate system settings, or execute malicious activities within the compromised system. These attacks pose a

significant risk to the confidentiality, integrity, and availability of the targeted system and the data it contains. To defend against R2L attacks, organizations and system administrators employ robust security practices. This includes implementing strong access controls, enforcing password policies, regularly updating and patching software and systems, and utilizing intrusion detection and prevention systems (IDS/IPS). Additionally, educating users about secure practices, such as avoiding suspicious emails or downloading files from untrusted sources, can help mitigate the risk of R2L attacks. Continuous monitoring and logging of network activities can aid in detecting and responding to R2L attacks in a timely manner. It is essential for organizations to have an incident response plan in place to swiftly address any potential breaches and minimize the impact of R2L attacks on their systems and data. By implementing proactive security measures, maintaining up-to-date software and systems, and promoting user awareness, organizations can strengthen their defenses against R2L attacks and protect their systems from unauthorized access and potential compromise.

The dataset contains a total of 125,943 connections and 41 characteristics. In some cases, the diverse nature of qualities observed in nature makes it difficult to apply certain machine learning methods. Creating a model becomes particularly challenging when dealing with continuous attributes. In order to enhance the accuracy of predictions, it is crucial to perform preprocessing before developing categorization patterns. To overcome this challenge, a discretization approach is specifically employed. Discretization, a data mining technique, aims to reduce the number of values for a continuous variable by organizing them into intervals. The literature offers two types of discretization methods that can be utilized.

Static variable discretization: The process of discretization is applied individually to each variable, without considering any dependencies or interactions with other variables. This approach ensures that each variable is discretized based on its own characteristics and distribution.

Dynamic variable discretization: In dynamic variable discretization, all attributes or variables are discretized simultaneously. This means that the discretization process takes into account the relationships and dependencies between variables, allowing for a more comprehensive and accurate representation of the data. In our study, apart from discretizing the assaults, we also

organized the attacks into groups based on their primary attack categories, namely DDoS, Probe, U2R, and R2L.

Performance metrics for comparison: The selection of appropriate performance metrics plays a crucial role in effectively evaluating intrusion detection systems (IDSs). As evaluating IDSs poses a significant challenge, it is essential to choose metrics that can accurately convey the quality and effectiveness of the system. While categorization rate is an important aspect of IDS performance, it is not the sole determinant. Therefore, we consider multiple performance measures to assess our system, including model precision, detection rate, cost per example (CPE), and overall detection rate. By considering a combination of these measures, we gain a comprehensive understanding of the system's performance.

Pre-processing, feature selection, and classification: To ensure optimal classification results, we propose a multi-step approach that involves pre-processing the entire dataset, selecting relevant features, and applying various classification algorithms. In the initial stage, we pre-process the dataset, which includes tasks such as data cleaning, normalization, and handling missing values. Following pre-processing, we employ feature selection techniques to identify the most informative and relevant features for the classification task. Finally, we utilize a range of classification algorithms, including J48, Bayes Net, Random Forest, and Hoeding Tree, toclassify the data. The performance of each algorithm is evaluated, and the best-performing algorithm is chosen for further analysis.

Back-propagation technique: In our research, we explore the application of a backpropagation learning algorithm in conjunction with a multilayer neural network for intrusion detection. The multilayer neural network comprises three layers: the input layer, the hidden layer, and the output layer. The input layer consists of 41 inputs, corresponding to the dataset features. The hidden layer, employed during the learning process, facilitates the network's ability to capture complex patterns and relationships within the data. For this technique, we utilize a single hidden layer with 100 neurons, which has been determined through empirical experience. Extensive experimentation has shown that different configurations of neurons and hidden layers do not significantly reduce the Mean Squared Error (MSE), leading us to adopt this specific configuration.

Distributed classification system: Our proposed approach involves a distributed classification

system, wherein each attack type (DDoS, Probe, R2L, and U2R) is assigned to the JRip algorithm. Subsequently, the models generated by each algorithm are combined using the AdaBoost technique. This distributed approach allows for efficient and effective classification, asit leverages the strengths and capabilities of multiple algorithms while benefiting from the collective knowledge obtained from each model. The AdaBoost technique enhances the overall performance of the classification system by assigning appropriate weights to each individual model, effectively combining their outputs to achieve accurate and reliable results.

3.2 Anomaly-Based Intrusion Detection

The installation and evaluation of our AI framework for identifying cyber-attacks based on anomalous behaviors in IoT systems are described in this section. Our framework leverages the temporal-spatial correlation between sensor data to detect potential hazards. Unusual sensor values can indicate attacks, malware infections, or man-in-the-middle impersonation of IoT devices. Specifically, our AI-based framework focuses on identifying faulty IoT devices and implementing reactive countermeasures. It is important to note that although not within the scope of this study, our system, when tested in a smart building testbed scenario, incorporates new traffic filtering rules using SDN to mitigate malicious traffic. Additionally, it reconfigures the vAA (virtual authentication agent), enables vChannel Protection for secure DTLs connections, and enforces the turn-off and/or flashing of IoT devices. These reactive countermeasures are being developed and tested as part of the Anastacia EU project and are beyond the scope of this research, which primarily focuses on evaluating machine learning algorithms for identifying cyber-attacks in IoT systems.

Data Collection: For our research, we collected a dataset comprising actual sensor data from four distinct rooms in our smart building testbed. Over the course of a month, we recorded CO2 and temperature readings from each room at two-minute intervals. The dataset consists of 67,876 samples representing normal values and includes characteristics such as ID, room, CO2 sensor value, temperature sensor value, and an optional class label. We created separate models for each sensor, taking into account temperature and CO2 measurements. While the CO2 levels varyacross rooms, the temperature remains consistent, suggesting the possibility of using the same model for all rooms.

Datasets:

- **Single Value Dataset (SV):** This straightforward dataset includes captured sensor values and timestamps as features.
- **Previous Five Values Dataset (P5V):** This dataset captures the temporal correlation between collected sensor data. It includes prior values from other datasets, such as date, value, precedent value, second precedent value, and fifth precedent value. We focused on the Room 1 dataset to simplify the analysis and reduce complexity.
- **Previous Different Three Values Dataset (PD3V)**: Similar to the previous strategy, this dataset considers the time correlation by only including the latest three distinct values: date, value, value difference precedent, second different precedent, and third different precedent, to

avoid duplication.

- **Cross Rooms Dataset:** This technique combines the room values to identify abnormalities, considering the correlation in sensing data across all rooms. By combining the data from all four rooms, we aim to enhance accuracy. The resulting dataset includes features such as date, label, rooms 1, 2, 3, and 4.

One-class SVM model: We developed and customized a one-class support vector machine (SVM) model using the Python Scikit-learn library to effectively detect anomalies in the dataset. The anomaly-based IDS approach consists of four steps. First, the dataset is cleaned and preprocessed. Then, data discretization is performed to transform the continuous time-series into discrete intervals. The learning algorithm is implemented, followed by the classification step of the search process. We used the values from the first room for training and the second room for testing in the temperature dataset. Additionally, we compared the model's performance with another room using CO2 data, as we observed a geographical association primarily with temperature data. The detection accuracy of the training dataset was assessed at 33 percent.

CHAPTER 4

Results Discussion

The results presented in Table 1 provide insights into the performance of different machine learning algorithms in detecting and classifying attacks. Among these algorithms, the Random Forest algorithm demonstrates favorable results in terms of overall accuracy and sample accuracy. It performs well in identifying various types of attacks, except for U2R (User to Root) and R2L (Remote to Local) attacks, where its performance is relatively limited.

	J48	Byes Net	RandomForest	Hoeffding Tree
DoS	99.9%	99.9%	100%	99.3%
U2R	70.0%	4.8%	82.1%	11.5%
U2L	97.5%	62.7%	99.3%	35.2%
Probe	99.4%	84.2%	99.9%	98.1%
Normal	99.8%	97.3%	99.9%	95.2%
Time(s)	35.35	6.97	74.94	5.1
Precision	99.8%	96.7%	99.9%	96.4%
FPR	0.2%	1.8%	0.1%	3.3%
Detection Rate	99.8%	95.7%	99.9%	96.8%
CPE	0.47%	6.8%	0.23%	7.46%

Table 1: Detailed Precision Values for Each Attack

On the other hand, the J48 algorithm showcases high accuracy and low latency (or CPE) in detecting attacks. It proves to be a useful tool in identifying most types of attacks, except for U2R attacks where its accuracy falls short. Despite this limitation, the J48 algorithm stands out due to its quick response time.

The Hoeffding tree algorithm exhibits stable performance across different attack types, but like the previous algorithms, it struggles with accurately detecting U2R attacks. This indicates a common challenge in effectively identifying U2R attacks across multiple algorithms.

In contrast, the Bayesian Network algorithm yields poor results, even with a high-fidelity

model. It fails to recognize the majority of U2R attacks, highlighting its limitations in this specific domain.

The Backpropagation system shows a slight improvement in accuracy compared to the previous method described in Table 2. However, it comes with a trade-off, as the misclassification rate is relatively higher when considering the runtime of the system.

	DoS	U2R	U2L	Probe	Normal	Model
Precision	99.1%	0%	81.6%	99.1%	98.7%	98.7%
FPR	0.5%	0%	0.1%	0.1%	1.5%	1.0%
Detection Rate	99.0%	0%	71.5%	98.9%	99.0%	98.7%
CPE	-	-	-	-	-	2.78%
Time(s)	-	-	-	-	-	9691.01

Table 2: Back-Propagation Evaluation Metrics

Moving on to Table 3, it showcases the performance of a newly developed system in comparison to the previous one. This new system exhibits notable improvements in terms of detection accuracy, accuracy, detection rate, and cost per sample (CPE). These enhancements signify the effectiveness of the newly implemented system in detecting and classifying attacks.

Table 3: Results Comparison with Previous Work

	Accuracy	Detection rate	FPR	Training Time
L-SSVM [38]	92.29%	92.2%	0.41%	-
DMM [39]	97.8%	97.8%	2.5%	-
TANN [40]	96.91%	97.8%	2.5%	-
DBN [41]	97.45%	-	-	3.2 sec
RNN [42]	99.53%	97.09%	3.6%	5516 sec
DNN [43]	75.75%	75%	15%	-
E-DNN [44]	92.49%	98%	14.7%	-
DFF-NN [45]	98.6%	99%	1.8%	398 sec
DL [46]	98%	71%	-	-
SVM-DR [46]	97.61%	97.27%	-	-
Our Approach1	99.8%	98.8%	0.2%	35.35
Our Approach2	98.7%	98.7%	1.0%	9691.01
Our Approach3	99.9 %	98.9%	0.1	193.6

To provide a comprehensive evaluation, the results in Table 3 are compared with recent studies focusing on accuracy, detection rate, negative rate, and CPE. Various systems are included in this comparison, such as Filter-Based Support Vector Machines (F-SVM), Dirichlet Mixture Models (DMM) [39], Triangular Neighborhood Networks (TANN) [40], Neighboring Networks (DBNs), Relational Neural Networks (RNN), deep neural network (DNN) Ensemble-DNN, and size reduction based on support vector machine.

Based on the benchmark results, the system based on the distributed JRip algorithm combined with the aggregation method emerges as the most effective solution. It outperforms the other systems included in the study, demonstrating its superiority in detecting and classifying attacks. However, it's worth noting that the other systems in the comparison also show promising results and are worthy of consideration in specific contexts.

In conclusion, the presented research sheds light on the performance of various machine learning algorithms in the domain of attack detection and classification. It highlights the strengths and weaknesses of each algorithm and presents a newly developed system that exhibits significant improvements over its predecessor.

The comparison with recent studies provides valuable insights into the competitive landscape and showcases the superiority of the distributed JRip algorithm with the aggregation method.

CHAPTER 5

Conclusion and Future Scope

5.1 Conclusion

In an increasingly connected world, where IoT systems are expected to transform our daily lives, ensuring the security of these interconnected devices is of paramount importance. In this article, we explored the most common threats to IoT systems and proposed a security framework that integrates Software-Defined Networking (SDN), Network Function Virtualization (NFV), and learning solutions.

The proliferation of IoT devices has opened up new attack vectors, making it essential to understand and address the potential risks. Unauthorized access, data privacy and integrity concerns, denial-of-service attacks, and the formation of botnets are among the significant threats faced by IoT systems.

To combat these threats, the integration of SDN, NFV, and learning solutions offers a promising approach. SDN allows for centralized management and control of the network infrastructure, enabling security policies to be enforced consistently across the IoT ecosystem. This centralized control also enhances visibility, making it easier to detect and respond to potential security breaches.

NFV complements SDN by virtualizing network functions, making it more efficient to deploy and scale security measures. This flexibility allows organizations to dynamically allocate resources and adapt to evolving security challenges. Additionally, NFV enables the implementation of security measures at various points within the network, including at the edge, where IoT devices often reside.

The incorporation of learning solutions, such as machine learning and artificial intelligence, further enhances the security framework. These technologies enable intelligent analysis of vast amounts of data generated by IoT devices, facilitating the

identification of anomalies and the detection of sophisticated threats. By continuously learning from patterns and behaviors, these solutions can proactively respond to emerging threats and prevent potential breaches.

Implementing a comprehensive security framework for IoT systems entails a multi-layered approach. Strong access controls, secure authentication protocols, end-to-end encryption, and regular security audits are vital components of this framework. Real-time monitoring of device behavior and network traffic helps identify suspicious activities, enabling rapid response and mitigation of potential threats.

However, it is essential to recognize that IoT security is an ongoing challenge. As technology evolves, new vulnerabilities and attack vectors will emerge. Therefore, a proactive approach to security is necessary, involving regular updates, patches, and vulnerability assessments. Collaboration between industry stakeholders, governments, and security experts is crucial to staying ahead of potential threats and ensuring the resilience of IoT systems.

In conclusion, as IoT systems become increasingly integrated into our lives, securing these interconnected devices is of paramount importance. By leveraging technologies likeSDN, NFV, and learning solutions, organizations can establish a robust security framework that mitigates common threats and safeguards the integrity, privacy, and functionality of IoT systems. Embracing these advancements in IoT security will empower us to fully harness the benefits of this transformative technology while effectively countering the evolving cybersecurity landscape.

We also present a case study demonstrating the feasibility of our AI-based security program that combines cognitive and intrusion detection. On the one hand, in terms of cognitive search, three different systems were used to evaluate methods based on the NSL KDD dataset:

1. System-based classification algorithms,

2. JRip algorithms based on division by union law, and some, such as

3. Discrimination backpropagation process

The results obtained are very useful, the assessment allows us to evaluate the quality of the framework and take into account the impact of unfair attacks. On the other hand, our framework integrates an IDS with single-level SVM for anomaly detection of sensor data, and the detection accuracy is higher than 98 percent for most of the combined dataset ideas.

Below we describe some additional research challenges that our security framework must address. First, we address the challenge of determining the connectivity model to facilitate interaction of the negotiation model, including the language used for the promotion of IoT security policies that should be based on AI decision making. Second, as the IoT landscape continues to evolve, AI systems will need to adapt to emerging (and perhaps unknown) IoT cyber-attacks that do not follow previous network/system signature and standards. Third, another challenge involves machine learning techniques and algorithms that operators can use to plan the best attacks to follow different contexts. Finally, we also pointed out that the security implementation is somehow related to the use of additional resources and poor performance; therefore, the balance between security and quality of service should be analyzed in depth in reactive models.

5.2 Future Scope

The integration of Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Artificial Intelligence (AI) with a Machine Learning (ML) Security Framework for IoT Systems holds significant potential for enhancing the security andresilience of IoT environments. The future scope of this integrated approach can be outlined as follows:

1. Enhanced Threat Detection: By leveraging SDN and NFV capabilities, along with ML and AI algorithms, the security framework can improve the detection of sophisticated and evolving threats in real-time. SDN can enable dynamic network monitoring and traffic analysis, while NFV can facilitate the deployment of virtualized security functions.ML and AI algorithms can analyze network traffic patterns, device behavior, andsystem anomalies to identify potential threats accurately.

2. Proactive Defense Mechanisms: Integrating ML and AI with the security framework can enable proactive defense mechanisms that can anticipate and prevent attacks before they occur. ML algorithms can continuously learn from historical data and security incidents to predict potential threats and vulnerabilities. AI techniques, such as reasoning and decision-making models, can provide automated response mechanisms, including adaptive security policies, threat mitigation strategies, and real-time incident response.

3. Context-aware Security Policies: SDN's programmability combined with ML and AI can enable the development of context-aware security policies tailored to the specific needs of IoT systems. The security framework can learn the normal behavior of IoT devices, network traffic patterns, and user activities, allowing it to dynamically adapt security policies based on the context. This ensures that security measures are effective while minimizing false positives and false negatives.

4. Threat Intelligence and Collaboration: ML and AI techniques can enable the security framework to leverage threat intelligence from various sources, such as security vendors, research institutions, and global security communities. By continuously learning from emerging threats and attack patterns,the framework can

improve its threat detection and prevention capabilities. Additionally, the framework can facilitate collaborative security efforts by sharing threat intelligence and security insights with other IoT systems, contributing to a more robust security ecosystem

5. Privacy and Data Protection: With the increasing concerns around privacy and data protection in IoT systems, the integrated security framework can incorporate ML and AI algorithms to ensure secure data handling and privacy preservation. ML techniques, such as federated learning and homomorphic encryption, can enable analysis and decision-making without compromising the privacy of sensitive IoT data. SDN and NFV can also facilitate fine-grained access control and data encryption mechanisms, ensuring data confidentiality and integrity.

6. Adaptive Network Resilience: By combining SDN, NFV, ML, and AI, the security framework canenhance the resilience of IoT networks against various cyber threats and attacks. ML algorithms can detect and respond to network anomalies and system failures, triggering SDN-based network reconfiguration and NFV-based service migration to maintain system availability and performance. AI-based resilience mechanisms can learn from past incidents and proactively adapt the network infrastructure to minimize the impact of security breaches.

7. Scalability and Flexibility: The use of SDN and NFV in combination with ML and AI offers scalability and flexibility in deploying security functions in IoT environments. SDN's centralized control and NFV's virtualized network functions can efficiently allocate and scale security resources based on the changing demands of IoT systems. MLalgorithms can adapt and optimize security mechanisms dynamically, ensuring efficient resource utilization and reducing the overall system overhead.

In conclusion, the future scope of a Machine Learning Security Framework for IoT Systems using SDN, NFV, and AI encompasses advanced threat detection, proactive defense mechanisms, context- aware security policies, scalability, flexibility, threat intelligence,

privacy protection, and adaptive network resilience. The integration of these technologies hold great promise for addressing the evolving security challenges in IoT environments and ensuring the secure and reliable operation of IoT systems.

Tarun_Report_plag

ORIGINALITY REPORT

14%	12%	11%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.mosaic-lab.org Internet Source	6%
2	Submitted to The University of Wolverhampton Student Paper	1%
3	acris.aalto.fi Internet Source	1%
4	Miloud Bagaa, Tarik Taleb, Jorge Bernal Bernabe, Antonio Skarmeta. "A Machine Learning Security Framework for IoT Systems", IEEE Access, 2020 Publication	1%
5	www.researchgate.net Internet Source	1%
6	dokumen.pub Internet Source	<1%
7	Submitted to Florida International University Student Paper	<1%
8	www.mdpi.com Internet Source	<1%

9	ebin.pub Internet Source	<1 %
10	Jing Yang, Yen-Lin Chen, Lip Yee Por, Chin Soon Ku. "A Systematic Literature Review of Information Security in Chatbots", Applied Sciences, 2023 Publication	<1 %
11	www.coursehero.com Internet Source	<1 %
12	ftp.ring.gr.jp Internet Source	<1 %
13	speakers.acm.org Internet Source	<1 %
14	ijns.jalaxy.com.tw Internet Source	<1 %
15	link.springer.com Internet Source	<1 %
16	secc.org.eg Internet Source	<1 %
17	1library.net Internet Source	<1 %
18	Submitted to University of Salford Student Paper	<1 %
19	abdulkamal3.wordpress.com Internet Source	<1 %

20	dspace.dtu.ac.in:8080 Internet Source	<1 %
21	careers.fairfaxtimes.com Internet Source	<1 %
22	core.ac.uk Internet Source	<1 %
23	docshare.tips Internet Source	<1 %
24	www.miun.se Internet Source	<1 %
25	fenix.tecnico.ulisboa.pt Internet Source	<1 %
26	hack4net.github.io Internet Source	<1 %
27	Aditya Harbola, Jyoti Harbola, Kunwar Singh Vaisla. "Improved Intrusion Detection in DDoS Applying Feature Selection Using Rank & Score of Attributes in KDD-99 Data Set", 2014 International Conference on Computational Intelligence and Communication Networks, 2014 Publication	<1 %
28	Miloud Bagaa, Tarik Taleb, Jorge Bernal Bernabe, Antonio Skarmeta. "A Machine	<1 %

Learning Security Framework for Iot Systems", IEEE Access, 2020

Publication

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Tarun_Report_plag

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35