



**KIET**  
**GROUP OF INSTITUTIONS**  
*Connecting Life with Learning*



**A**  
**Project Report**  
on  
**A Security Infrastructure for IoT Devices**  
**based on Machine Learning**  
submitted as partial fulfillment for the award of  
**BACHELOR OF TECHNOLOGY**  
**DEGREE**

SESSION 2022-23  
in  
**Computer Science and Engineering**

By  
Tarun Kumar (1900290100171)  
Shraddha Singh (1900290100147)  
Shubham Bhaskar (1900290100156)  
Piyush Mishra (1900290400081)

**Under the supervision of**

Ms. Himanshi Chaudhary

**KIET Group of Institutions, Ghaziabad**

Affiliated to  
**Dr. A.P.J. Abdul Kalam Technical University, Lucknow**  
(Formerly UPTU)

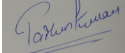
## DECLARATION

We hereby declare that this submission is our own work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Name: Tarun Kumar

Roll No.: 1900290100171


Date: 31/05/2023

Signature : 

Name: Shraddha Singh

Roll No.: 1900290100147

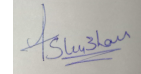
Date: 31/05/2023

Signature : 

Name: Shubham Bhaskar

Roll No.: 1900290100156

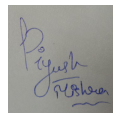
Date: 31/05/2023

Signature : 

Name: Piyush Mishra

Roll No.: 1900290400081

Date: 31/05/2023

Signature : 

## **CERTIFICATE**

This is to certify that Project Report entitled “A Security Infrastructure for IoT Devices based on Machine Learning” which is submitted by Tarun Kumar, Shraddha Singh, Shubham Bhaskar, Piyush Mishra in partial fulfillment of the requirement for the award of degree B. Tech. in Department of Computer Science & Engineering of Dr. A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

**Date:** 31/05/2023

**Supervisor Name**

Ms. Himanshi Chaudhary

## ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B. Tech Project undertaken during B. Tech. Final Year. We owe special debt of gratitude to Ms. Himanshi Chaudhary, Department of Computer Science & Engineering, KIET, Ghaziabad, for their constant support and guidance throughout the course of our work. Their sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavors have seen the light of the day.

We also take the opportunity to acknowledge the contribution of Dr. Vineet Sharma, Head of Department of Computer Science & Engineering and Dr. Ashish Karnwal, Head of Department of Mechanical Engineering, KIET, Ghaziabad, for their full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the faculty members of the department for their kind assistance and cooperation during the development of our project.

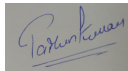
We also do not like to miss the opportunity to acknowledge the contribution of all faculty members, especially faculty/industry person/any person, of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

Name: Tarun Kumar

Roll No.: 1900290100171

Date: 31/05/2023

Signature:

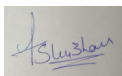


Name: Shubham Bhaskar

Roll No.: 1900290100156

Date: 31/05/2023

Signature:



Name: Shraddha Singh

Roll No.: 1900290100147

Date: 31/05/2023

Signature:



Name: Piyush Mishra

Roll No.: 1900290400081

Date: 31/05/2023

Signature:



# ABSTRACT

The rapid growth of Internet of Things (IoT) devices has led to an increased demand for robust security measures to protect the vast amounts of sensitive data transmitted and stored by these devices. Machine learning (ML) techniques have shown promising potential for enhancing the security infrastructure of IoT devices. This literature review aims to explore the existing research on the development and application of ML-based security solutions for IoT devices.

Both academic and business communities are paying increasing attention to Internet of Things security. IoT devices are in fact vulnerable to a variety of security assaults, including Denial of Service (DoS) attacks, network intrusions, and data leaking. This study introduces a brand-new machine learning (ML)-based security framework that adapts automatically to the evolving security needs of the IoT domain. For the purpose of reducing various vulnerabilities, this framework makes use of both Software Defined Networking (SDN) and Network Function Virtualization (NFV) enablers.

This AI framework combines a monitoring agent with an AI-based reaction agent that analyses network patterns using ML-Models and detects intrusions into IoT devices based on anomalies. To accomplish its objectives, the framework makes use of supervised learning, a distributed data mining system, and neural networks. Results from experiments show how effective the suggested plan is. In particular, the data mining technique to attack distribution is quite effective in identifying attacks with high performance and cheap cost.

We used one-class SVM to assess the experiment for our anomaly-based intrusion detection system (IDS) for the Internet of Things in a real Smart building scenario. The detection of anomalies was 99.71% accurate. A feasibility study is carried out to determine the present viable solutions that could be used and to encourage research into the unresolved problems.

# TABLE OF CONTENTS

Page No.

DECLARATION.....	ii
CERTIFICATE.....	iii
ACKNOWLEDGEMENTS.....	iv
ABSTRACT.....	v
LIST OF FIGURES.....	vi
CHAPTER 1 (INTRODUCTION).....	9
1.1. Introduction.....	9
1.2. Infrastructure Description.....	11
1.3. Background of Technologies.....	21
CHAPTER 2 (LITERATURE REVIEW) .....	25
CHAPTER 3 (PROPOSED METHODOLOGY) .....	27
3.1. Network Pattern Analysis.....	27
3.2. Anomalies Based Intrusion Detection.....	33
CHAPTER 4 (RESULTS AND DISCUSSION) .....	35

CHAPTER 5 (CONCLUSIONS AND FUTURE SCOPE) .....	38
5.1. Conclusion.....	38
5.2 Future Scope.....	41
APPENDIX (RESEARCH PAPER) .....	43
REFERENCES.....	49

## LIST OF FIGURES

Figure No.	Description	Page No.
1(a)	General Architecture of Infrastructure	11
1(b)	Closed Loop Automation	12
2	Overview of the interactions between the components of AI-based Security framework for IoT Systems	17



# 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 introduction of new services and capabilities in IoT technology introduces unseen vulnerabilities, making the task 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.

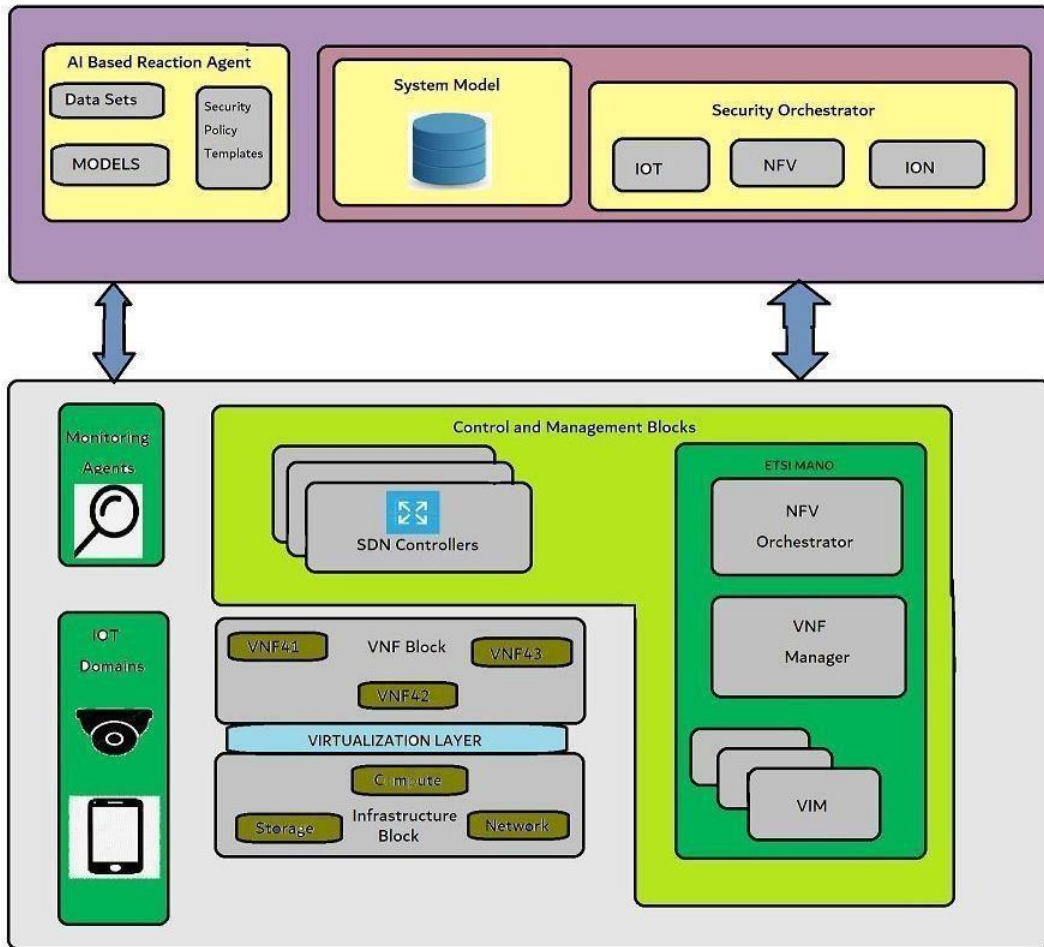


Figure-1(a) General Architecture of Infrastructure

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. ML algorithms analyze the collected data, identifying potential threats and alerting the security operators.

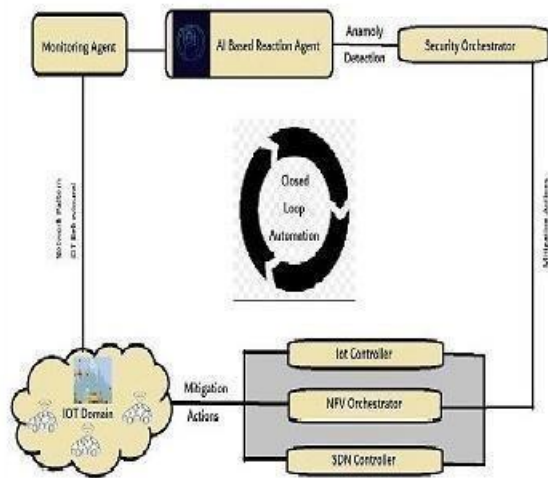


Figure-1(b) Closed Loop Automation

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. External attacks 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, such as 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 network services. 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 and countermeasures 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 as security 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, and monitoring 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.

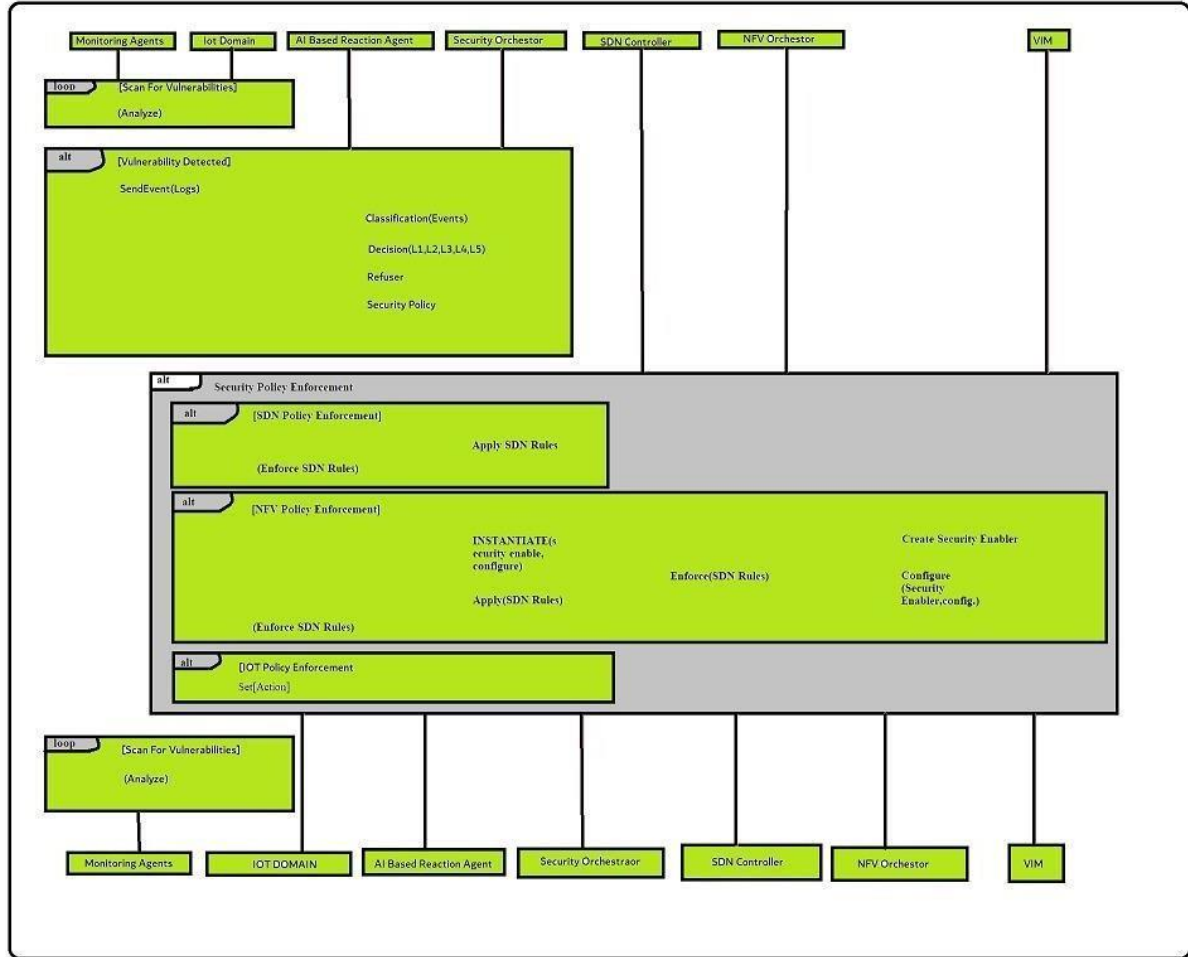


Figure 2 Overview of the interactions between the components of the AI-based Security Framework for IoT Systems.

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 respond proactively.

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 approach strengthens 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, enabling researchers 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 and reliability 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 response phases. 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 gain unauthorized 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 system configurations, 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 strong access 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, to classify 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, as it 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 CO<sub>2</sub> 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, CO<sub>2</sub> sensor value, temperature sensor value, and an optional class label. We created separate models for each sensor, taking into account temperature and CO<sub>2</sub> measurements. While the CO<sub>2</sub> levels vary across 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 like SDN, 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 and resilience 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, and system 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 can enhance 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. ML algorithms 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.

## APPENDIX

# A Security Infrastructure for IoT Devices Based on Machine Learning

Tarun Kumar

*Student, CSE Department  
KIET Group of Institutions  
Delhi-NCR, Ghaziabad, India  
tarun.1923cs1118@kiet.edu*

Shraddha Singh

*Student, CSE Department  
KIET Group of Institutions  
Delhi-NCR, Ghaziabad, India  
shraddha.1923cs1193@kiet.edu*

Shubham Bhaskar

*Student, CSE Department  
KIET Group of Institutions  
Delhi-NCR, Ghaziabad, India  
shubham.1923cs1031@kiet.edu*

Piyush Mishra

*Student, CSE Department  
KIET Group of Institutions  
Delhi-NCR, Ghaziabad, India  
piyush.1923me1141@kiet.edu*

Himanshi Chaudhary

*Assistant Professor, CSE Department  
KIET Group of Institutions  
Delhi-NCR, Ghaziabad, India  
himanshi.chaudhary@kiet.edu*

**Abstract**—Academic and industrial interest in IoT security is expanding. IoT devices are vulnerable to DoS, network infiltration, and data leaking attacks. This study introduces an ML-based security framework that automatically handles IoT security issues. This framework mitigates vulnerabilities using SDN and NFV enablers. This AI framework uses ML-Models for network pattern analysis and anomaly-based intrusion detection in IoT devices to monitor and react. The approach uses supervised learning, distributed data mining, and neural networks. Experiments show the scheme's efficiency. The data mining approach detects assaults with great performance and minimal cost. Our anomaly-based IoT intrusion detection system (IDS) was tested in a real Smart building scenario utilising one-class SVM. 99.71 percent of abnormalities were detected. A feasibility study identifies current solutions and promotes research on open challenges.

### I. INTRODUCTION

The rapid impact of IoT [1] is changing the current ICT landscape, as we expect the emergence of various IoT mobile devices in the coming years. IoT devices are used in many ways in our lives today. B. Medical care, transportation, home environment. Thanks to the great progress in analytics and cloud computing technology, we will hopefully be able to use direct communication to provide relevant information and content without affecting people. The swift adoption of this technology is attributed to its numerous benefits. However, IoT nodes are susceptible to targeted attacks by malevolent actors who exploit their limited resources and vulnerabilities. The pervasiveness of IoT security threats raises concerns about privacy infringement and financial losses. As these devices become an integral aspect of our everyday lives, it is

crucial to prioritize privacy, security, and job protection. For instance, IoT devices are employed in various domains such as healthcare and manufacturing and may contain sensitive personal information, including data usage and daily activities.

Breaches on these devices can result in the exposure of private data, interfere with operations, and impact product quality. To address the limitations and shortcomings of IoT systems, software-based networking seems most attractive solution. The integration of cloud computing and software models with network services is a promising new the mostly known as network software. This technology aims to improve business performance significantly. Network software involves two different approaches: SDN and NFV. SDN isolates the control and data planes, which results in a new level of network performance. A central logic controller monitors network conditions and assigns rules to network elements to manage traffic effectively. NFV, on the other hand, employs virtualization technology to provide network content as a software instance, thereby increasing the flexibility of service delivery. NFV can also reduce CAPEX/OPEX costs by substituting costly hardware with external servers that can host a software-based network.

SDN and NFV are two separate concepts, but when used together they can enhance security services from the network to meet the many needs of IoT. Increasing demand for IoT devices, location in mobile gaming apps, and haptic web apps are prime examples of advanced situations that introduce many new vulnerabilities and technical issues.

exposing hidden forms of vulnerabilities. Machine learning is really challenging in this situation. Modern AI systems use machine learning to categorize assaults as dangers and identify them [2].

Deep machine learning policies may also be adjusted over time when they are integrated into networks, giving network administrators a powerful deterrence against hackers. Contrary to conventional approaches, IoT entry must take process metrics into account in addition to communication data.

This document presents a complete methodology for detecting and preventing cybersecurity attacks [3] in 5G networks by leveraging machine learning (ML) techniques with SDN, NFV, and IoT controllers. Several contributions were made to this paper:

- An integrated artificial intelligence security framework that follows the ETSI ZSM vision by automatically, independently, autonomously and collaboratively monitoring, detecting and preventing cybersecurity threats.
- Artificial Intelligence Security framework for the Internet of Things is implemented and implemented, using machine learning techniques to control information understanding based on uncertainty not only from the network signature / authentication model, but also from normal behavior, reporting content for data analysis, with tracking capacity framework;
- Our Sunar Methodology uses Machine Learning Methods to identify Cybersecurity attacks based on network models;
- An integrated AI security framework can identify new types of cyber attacks that cannot be detected by known network models (0-day attacks) in IoT. The use of SDN/NFV-based security management can effectively and efficiently mitigate cyberattacks based on core thinking-driven AI-driven decision-making.

## II. RELATED WORK

Many books and articles have been written about the crucial subject of Internet of Things security. One of them suggests an Internet of Things security framework tailored to smart buildings, with a focus on capturing operational data from sensors to identify any suspicious activity in the IoT domain. The data is then used to locate sensors whose behaviour deviates from the "normal" behaviour. The framework flags suspicious activity and triggers recovery procedures like re-authenticating sensors, transmitting sensor data, and updating network settings if an attack is detected. Results reveal the system can reliably detect assaults, however it has a low attack reduction rate, which frequently causes service disruptions. Also, all of the IoT framework's layers are vulnerable to attacks because the framework doesn't offer end-to-end (E2E) security.

The security policies for IoT networks are defined using several features of SDN (Software Defined Networking). Additional security measures, such as virtualization, traffic filtering, and network security for the delivery of sensitive

information, can be incorporated with the help of SDN technology. Research publications have focused on evaluating the performance and feasibility of running virtual security appliances at the edge using containers, such as intrusion prevention systems (IPS) and firewalls, in the context of NFV (Network Function Virtualization). The significant CPU and power consumption caused by the heavy traffic makes this lightweight virtualization technology difficult to execute for devices that are restricted to IoT applications. Machine learning is another option for protecting the Internet of Things. Various solutions have been proposed to facilitate access to the network using SDN technology and ML technology. The study also describes operational issues associated with using a network access detection system. The authors of offer a solution to predict city bus locations using deep learning. In the solutions, long-term memory (LSTM) [4] based neural networks are considered for local information and value estimation. The proposed method uses machine learning about trust and decision trees to detect different attacks. AI can use IoT intrusion detection systems (IDS) to detect malicious behavior based on coordination and physical metrics. Presented an artificial intelligence-based IDS approach for the Internet of Things [5] that uses correlation of time-series sensor data to identify suspected vulnerabilities. However, our AI framework is designed not only to check for bad IDSs, but also to recognize IDSs by constantly checking signatures and intelligence patterns and opposition. Know beforehand. In this context, most of the studies carried out to date have focused on the discovery phase of the phenomenon. When an attack is detected, our framework is designed to include a response phase. We firmly believe that the best solution would be to provide end-to-end security through a thorough discussion of the SDN checker and appropriate AI policy definition and development. This appropriate security policy will be enforced by the development capabilities provided by cloud-hosted virtual network security tools. That's why we started a new artificial intelligence-based security project for IoT systems.

## III. PROPOSED FRAMEWORK

### A. Background of Technologies

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, ac, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

#### 1) Software Defined Networking (SDN)

Software-defined networking (SDN) is an innovative method that separates the control plane from the data plane to improve network agility, efficiency, and administration. It also enables external applications to regulate network behavior and create micro-networks in a more streamlined and efficient manner. Additionally, SDN provides the capability to customize network traffic to meet application requirements. The three fundamental components of an SDN-enabled network

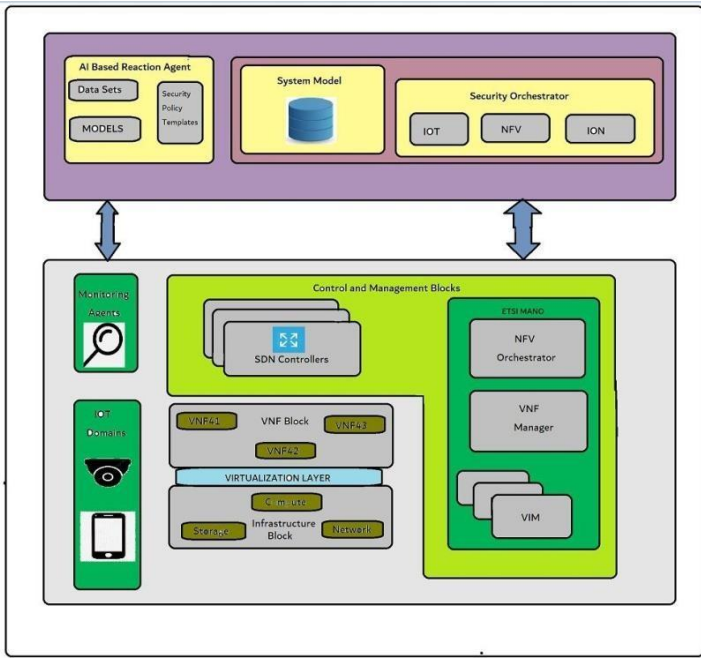


Fig. 1. Architecture of the Framework

include the switch, controller, and networking. The SDN controller plays a pivotal role in determining priority transmission and controlling all associated systems. For future IoT systems to be successful and sustainable, the incorporation of SDN into the design is essential. SDN's expertise in routing traffic and optimizing network usage is an attractive proposition for managing and monitoring big data traffic in IoT networks. This integration can take place at various levels of the IoT network, including the access layer (where data is generated), core network, and cloud network (where data is processed and analyzed), enabling end-to-end IoT traffic management. Furthermore, SDN can enhance IoT security by isolating traffic from different tenants, ensuring network consensus for security, and reducing traffic to prevent network-wide damage.

## 2) Network Function Virtualization

NFV is a network virtualization technology that provides high performance, significant capacity, and efficiency by separating software from hardware, unlike traditional network devices. The standard was created by ETSI, which defined new standards to achieve these results. The ETSI NFV Architecture consists of three primary elements.:

- Virtualization Infrastructure, which consists of all hardware and virtualization software needed to create Virtualized Network Functions (VNFs). This covers the computing, networking, and storage resources that cloud computing systems normally manage.
- Virtual Network Functions, which use VNF to replace the software version of network functions with special equipment. These can be used and controlled in many locations, providing efficient connectivity.
- Management and Monitoring, which addresses the pro-

tol and VNF layer within the ETSI NFV architecture. VNF manages the deployment in its entirety, including initialization, configuration, and maintenance. The rapid growth of IoT ecosystems can be attributed to the incorporation of virtualized network resources. This integration provides a number of benefits that contribute to their expansion. NFV provides sophisticated monitoring tools, such as intrusion detection (IDS) and deep packet inspection (DPI), security and authentication, personnel monitoring, and protection from attacks when combined with SDN.

- Additionally, installing additional security measures from resource constrained IoT devices to a virtual environment can save energy and increase efficiency by providing more slots for other useful applications. The convenience and enhanced security features of NFV are not currently available in current IoT security hardware. [5] Although NFV is not intended to replace existing IoT solutions, its additional benefits are attractive and revolutionary in the field of IoT security. machine learning technology.

## 3) Machine Learning Technique

Machine learning, also known as ML, is an area of artificial intelligence that focuses on giving computers and other smart devices the ability to learn on their own. In the field of network security, the machine learning approaches of supervised learning, unsupervised learning, and incremental learning are the ones that are utilised the most frequently [6]. These techniques are used to identify and specify safety rules for flight information. The primary challenge is to enhance the security mechanisms used to mitigate specific attacks by flagging network traffic or defining access control rules. Various machine learning techniques can solve many IoT attacks, such as neural networks, which can be used for network penetration and malware detection in DoS and K-NN attacks. One popular approach in machine learning is tracking learning, which involves learning from one dataset and evaluating the model with another dataset, even if the relationship between the data is unknown [7]. In the security context, this approach is useful for identifying attacks on groups of dissidents. Unsupervised learning, on the other hand, is different from supervised learning in that it does not require prior information about the model. Instead, it attempts to classify data into different groups based on the relationships between them. While, Reinforced learning focuses on learning problems and strategies to improve the bar. There is a certain way to train a model; It takes trial and error and is very effective. It monitors its output and uses rewards to calculate a value called a "value function". The model knows the accuracy of its decisions according to this value and adjusts accordingly.

## B. Framework Overview

Computing in the fog, also known as computing at the edge, can help speed up analysis and decision making for applications that are sensitive to latency. Before putting different applications and services into production, it is essential to evaluate their functionality as well as their level of performance.

### 1) Security Implementation plan

The second type of attack originates from the end user's external network and targets the IoT domain network, whereas the first type of attack results from incorrect IoT devices and intruders launching attacks against other legitimate IoT devices or networks. These attacks can target IoT devices through IoT controllers, network levels using SDN controllers, or Cloud/MEC levels using NFV orchestrators. To ensure secure IoT collection, the security tools outlined in the Framework should be implemented using secure VNFs and establishing connections over SDN networks. Specifications for ETSI NFV and ONF SDN have been incorporated into the architecture of the Protection Plane to ensure full compliance. The security protection concept includes three reasons.

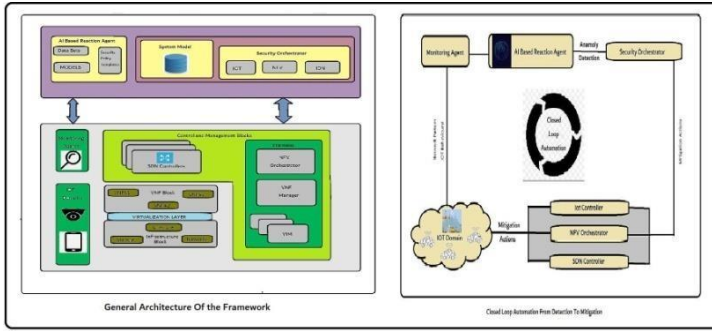


Fig. 2. Framework Overview

- **Virtual Network Function (VNF) Block** - The deployment of VNFs on virtualized infrastructure can enhance security through the use of various network services. To provide the necessary protection for personal information, particular attention should be given to deploying VNFs that offer better security features, such as virtual firewalls, IDS/IPS, and other relevant security measures.
- **Management and Control Blocks** - These blocks contain SDN/NFV management components. The SDN controller and ETSI MANA cluster module are included. NFV is often used with SDN to adapt the network based on resources and policies, therefore the NFV scheduler and SDN controller's interaction is crucial for deployment and security.
- **Infrastructure Block** - This block contains all the physical systems that offer computation, storage, and connection for an Infrastructure as a Service (IaaS) operation utilising relevant technologies. The plan also includes distributed security monitoring to gather data to support the components and monitoring services responsible for traffic management according to SDN rules.
- **Monitor** - The monitor is responsible for detecting various attacks by reporting network traffic and IoT behavior. In our proposed framework, the detection process utilizes both IoT behavior and network architecture, enabling operators to monitor all traffic on the network through SDN. An AI-based agent responds to any suspicious

activity by sending logs with a description of the event in compliance with aircraft safety regulations.

- **Internet of Things (IoT) Domain** - This domain represents a network of SDN-enabled physical devices, including security cameras, thermometers, home appliances, and other smart devices that exchange data. Due to the high risks associated with these devices, our framework aims to ensure security to safeguard the integrity and safety of the data.

### 2) Security Orchestration plan

This plane sets and refines security policies depending on audit data. This is a new layer in our department that is responsible for managing security policies in the IoT collection by creating security management requirements. This involves deploying, configuring, and monitoring a variety of virtual security measures in response to ongoing assaults. The main interactions can be seen in the diagram in Figure 2, which shows the various interactions between the three principles. This document introduces a closed-loop automation mechanism from a responsible, AI-based agent to a security guard. Second, it protects against threats posed by IoT Checker, SDN Checker, and NFV Dispatcher, in that order.

#### a. AI-BASED REACTION AGENT

This device warns the security administrator of security threats. As shown in Figure 1(B) and the first block of Figure 2, monitors capture network and IoT data. This component detects risks using network and IoT-trained machine learning models. Machine learning models recommend security requirements to the security manager. Figure 1(B) and the second block in Figure 2 show how IoT behaviour and network topology detect security concerns. Threats at each security policy level (L1, L2, L3, L4, L5) are discovered and reported to the security manager. AI-based reactive agents use J48, Bayesian network, random forest, Hoeffding, SVM, and deep learning to detect IoT-related behaviour differences, attacks, and network structure. Section IV will provide additional compliance guidance.

#### b. SECURITY ORCHESTRATOR

The AI Response Agent uses this product for closed-loop security policy management. SDN and NFV management and control blocks apply IoT security policies. In the third block of Figure 2, a security regulator can influence dangerous traffic by launching, configuring, and monitoring a virtual security appliance, utilising SDN to regulate traffic, or directly on the IoT device, such as shutting it down. a barrier. Security Orchestra also stores sample files containing all data plane and policy information such as reactive proxy requests, SDN controllers and switches, working VNFs, and their IoT device configurations and information.

### C. Implementation Tools

In this subsection, we make an assessment of the feasibility of our solution. For this purpose, we explain the necessity of opening the project used to do the planning process.

#### 1) ONOS SDN Controller



ONOS, an open-source project, is developing SDN capabilities for telecoms and service providers [8]. It excels in availability, scalability, and performance. Through its applications, it expresses traffic management using protocols like OpenFlow and NetConf. Excellent content and network information like available nodes, packet counts for specific streams, and linked availability help application development.

2) ETSI Open-Source Mano (OSM) OSM is a 2016 Mobile World Congress (WMC) NFV Orchestrator. Merantis, Telefonica, BT, Canonical, Intel, RIFT.io, Austria Telecom, and Telenor developed it together. OSM supports multi-cloud and SDN vendor support for OpenStack, AWS, ONOS, and Opendaylight, following the ETSI NFV MANO application architecture. Three main parts:

- The Service Orchestrator (SO) is responsible for end-to-end service organization and delivery, providing a web link and directory. Its description differs from that of NFV.
- The Resource Orchestrator (RO) is used to deliver services from an IaaS provider in one place. It interacts directly with the Virtual Infrastructure Manager (VIM) to instantiate virtual resources.
- The VNF Configuration and Abstraction (VCA) utilizes the Juju Charms LXD box to perform the initial configuration and maintenance of Virtualized Network Functions (VNFs).

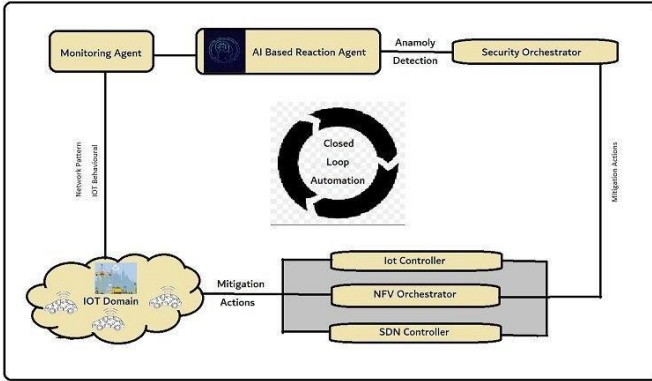


Fig. 3. Closed Loop Automation

#### IV. AI-BASED REACTION AGENT IMPLEMENTATION AND PERFORMANCE EVALUATION

The experiment design and assessment analysis of the AI-based reaction agent are provided in this section. An AI-based reaction agent analyses network patterns to find risks. A knowledge-based intrusion detection framework is suggested for i) analysing the anomalous behaviours in the IoT system and ii) detecting various network threats. In this section, the investigation of anomalous IoT system behaviours is used to identify cyberattacks.

In order to precisely categorise the severity of the threats and select the best security templates, we applied supervised

learning algorithms. The AI-based reaction agent will employ a variety of machine learning approaches to minimise a particular threat using the pertinent inputs from the monitoring agents.

##### A. Network pattern analysis

Evaluating the attack process helps prove the framework's efficacy. DARPA, KDD99, and DEFCON are popular for this. Neptune-dos, pod-dos, smurfdos, buffer-overflow, rootkit, demon, teardrop, etc. NSL KDD is an upgrade of the original Kdd99 file with serious flaws that could lead to poor IDS analysis, hence we designed an IDS based on it. According to the revised NSL KDD files, it addresses numerous important issues and removes 77 backlogs. We construct AI-based reactive agents using the NSL KDD dataset. We assessed IDS using the NSL-KDD dataset using Weka preprocessing and visualisation data mining. Weka classifies training models. The KDD dataset has 125,943 links and 41 signatures, each of which is involved in a denial of service (DoS), user-to-root (U2R), remote local stop (R2L), or stop tracking attack. Some machine learning algorithms can't learn from nature's variety. Fixed behaviour complicates design. Thus, the preliminary step precedes classification system development to get the right estimate. Decision-making resolves this restriction. Integrating discrete variables into an array reduces their number in data mining. Literature uses two discretization methods:

- Static variable discretization: discretization is done independently of other factors.
- Dynamic Variable Discretization: All variables are discretized concurrently.

We discretized and grouped the attacks by principal attack category (DDoS, Probe, U2R, and R2L).

- Penetration testing benchmarking is easy and should describe the IDS's strength. IDS functions go beyond classification. Our system was evaluated on sample accuracy, detection rate, precision, and cost per sample (CPE). It is a crucial parameter for determining an intrusion detection system's misclassification value, where CM is the distribution model's confusion matrix and C is the data processing value matrix. The sample is  $t$  and  $N$ . Below are some ideas. 10x cross validation on an i5-8350U with 16Go RAM evaluates our system.
- Preprocessing, feature selection, and classification: We propose preprocessing and then combining all the data using J48, Bayesian network, random forest, and anchor tree techniques. We pick the most efficient algorithm.
- Back Propagation Techniques: Below we examine neural network techniques using back propagation learning techniques. There are three layers in the multilayer neural network. There are 41 inputs (dataset features) in the input layer, the topmost layer. The final layer, which is a hidden layer that is included in the learning process, responds to classification (Dos, Probe, U2R, R2L, Values). We have taken into account a buried layer and 100 neurons in this process. These limitations are

considered useful, as other results of the latent system and the neuron number squared error (MSE) did not show significant improvements.

- However, it has little effect on U2R and R2L attacks. J48 detects attacks with high accuracy and low probability. However, the J48 is not very useful for U2R attacks in terms of accuracy. The performance of the Hoeffding tree algorithm is stable, but it also has the problem of low pressure of the U2R attack. In particular, the Bayesian Network algorithm showed poor results as it did not recognize most U2R attacks even with a high-fidelity model. Compared to the previous method, there is actually some improvement in the accuracy of the reverse method. However, the misclassification rate is somewhat high relative to the run time.
- AdaBoost received enhanced models in terms of detection rate, cost per example (CPE), accuracy, and precision.
- Comparative Analysis: The performance results are shown in the dataset results. This system obtained an improved model when compared to earlier systems in terms of detection rate, cost per example (CPE), accuracy, and precision.

We compare with recent studies based on accuracy, detection rate, negative rate, and CPE (if applicable). The results of the dataset provide an overview of recent work. The benchmark results show that our system-based distribution JRip algorithm and integration is at its best when the results from our other systems are equally supported. These systems include Dirichlet Mixture Model (DMM), Triangular Field Neighbor Network (TANN), Deep Belief Network (DBN), Ensemble DNN, Recurrent Neural Network (RNN), Deep Neural Network (DNN), and Filter-Based Support Vectors machine (F- SVM).

### B. Intrusion Detection Based on Anomalies

This section explains the accuracy of the study of abnormal behavior (variable sensor data) in IOT systems and the configuration and evaluation to find cyber probes. [9] AI projects have been proposed using spatio-temporal correlations of various sensor data to describe states. Negative sensitivity results may indicate that an IoT device has been compromised by hackers, malware, or a man-in-the-middle. Our IA-based framework detects IoT device failures and implements corresponding countermeasures. While this is beyond the scope of this article, when our framework is deployed in a smart home testbed scenario, plan mitigation i.e. 1) reconfiguration of vAAA (Virtual Authentication Agent), 2) Protection that helps vChannels to establish a secure DTL communication, 3) using new rules to filter traffic using SDN to mitigate weak tools; and 4) optionally shutting down and/or flashing IoT devices. The purpose of this article is the analysis of machine learning algorithms to detect cyber attacks in IoT systems, rather than reactive countermeasures developed and tested as part of the Anastacia AB project.

- Data collection: Actual sensor data from four separate rooms in our testbed for smart buildings were used to

produce the dataset for the study. Every two minutes for a month, we took temperature and CO2 readings in each room. The characteristics ID, Room, SensorValueCO2, SensorValueTemperature, and Class (Optional) are used to define the dataset, which includes measurements of 67876 samples that are thought to have normal values. Temperature and CO2 considerations have been built into models for each sensor. Given that the temperatures remain consistent throughout while the CO2 values vary for each room, the same model may be applicable to all of them. The first room might be used for testing, while others might be for training.

- Datasets:
  - Dataset containing a singular value (SV): It is a simple data collection consisting only of the captured value and the time as attributes for the created values.
  - Prior five values (P5V): This technique captures the temporal correlation between sensor data. Due to the contextual nature of temperature, this data set also incorporates information about earlier values from features in other datasets that are included in the single value data set. This dataset includes the five prior values for each value, including date, value, precedent value, second precedent value, and fifth precedent value. In addition, we have observed a significant correlation between these quantities.
  - Previous Different Three Values (PD3V): This strategy, like the preceding one, utilises the time correlation between the acquired sensor data. This method aims to avoid duplication by only considering the previous three distinct values [date, value, value difference precedent, second different antecedent, third different precedent] each time.
  - Cross-room correlation: The correlation has been taken into account in this method for sensing data in all rooms by combining room values to identify anomalies. Using this dataset, we aggregate the results for the four rooms in an effort to improve precision.
- One class-SVM model: Using Python's Scikit-learning tools, we wish to construct and edit a support vector machine class in order to create a model capable of identifying anomalies in data. We've suggested four stages for the standard IDS model [10]. First, the data are wiped clean. The second step, data discretization, entails converting continuous time values to discrete ones. The learning algorithm is used as the final search phase prior to the classification procedure. We classify the training results for the first grade and the test values for the second grade in the temperature data. We chose not to utilise data from other units to assess the CO2 data-based model because only the temperature data were correlated.
- Outcomes and contrast: The temperature test demonstrates that SV and P5V are more sensitive than other



combinations, with detection accuracy of 98 percent. The p5V data for 86 percent and CO2 reached 99.24 percent accuracy.

## V. FINAL THOUGHTS AND UNSOLVED RESEARCH PROBLEMS

We hope that IoT systems will soon change the way we live. Providing on demand security measures is one of the most valuable resources that can counteract the effectiveness of network protection. In our report, we explore the most dangerous aspects of IoT systems. We think that by combining SDN, NFV, and machine learning, a powerful security system that can enforce security policies can be produced. Another study demonstrates the viability of our AI-based security system combines knowledge-based and invisible detection. On the other hand, three more tasks were performed to evaluate the process based on NSL KDD knowledge about search information: Classification process based on:

1. classification algorithm
2. JRip algorithm, association rule
3. Including a back-and-Forth process and decision making.

We use several previous methods. The outcomes are really positive, and the standards enable us to accurately evaluate the framework and account for the impact of erroneous assaults. On the other hand, our system integrates IDS to detect if the sensor data is suspicious using single-stage SVM, which provides over 98

Additional research barriers that our security architecture aims to overcome are described below. In order to more easily see the interaction between the framework's models, we first address the problem of creating a connectivity model that includes the language used to express IoT security and the rules needed to respond to AI-based decisions. Second, because the Internet of Things landscape is constantly changing, AI systems must adapt to deal with new (and possibly undetected) IoT cyberattacks that do not follow network/system design marks and standards. Re-engineers who use machine learning techniques and algorithms to come up with the best plans for use in various situations are another challenge. Finally, we note that maintaining security levels requires additional resources and can lead to poor performance; therefore, recycling equipment must carefully consider the balance between safety and quality of service.

## REFERENCES

- [1] O. and F. P. Vermesan, "Internet of things: converging technologies for smart environments and integrated ecosystems.", River publishers., 2013.
- [2] R. R. V. P. R. and R. V. Prasad "Artificial intelligence and machine learning in cyber security". Cyber security: the lifeline of information and communication technology, pp. 231-247, 2020.
- [3] W. Z. P. H. K. and C. G. Zheng, "Understanding the property of long term memory for the LSTM with attention mechanism", In Proceedings of the 30th ACM International Conference on Information and Knowledge Management, pp. 2709-2717, October 2021
- [4] A. D. S. K. G. A. K. A. S. A. K. S. M. .. and. U. M. A. Singh, "Evolving long short-term memory network-based text classification.", Computational Intelligence and Neuroscience, 2022.
- [5] S. V. Thiruloga, "Anomaly Detection with Machine Learning for Auto- motive Cyber-Physical Systems (Doctoral dissertation, Colorado State University).", , 2022.
- [6] O. S. V. M. D. R. J. J. V. O. L. G. P. F. .. and F. M. Tătaru. "A Location- based service for handyman order placement", Diagnostics, vol. 2, no. 11, p. 354, 2021.
- [7] R. and Z. B. Bellazzi. "Predictive data mining in clinical medicine: current issues and guidelines", International journal of medical informatics, vol. 2, no. 77, pp. 81-97, 2008.
- [8] S. and P. S. N. Badotra. "" Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking", Cluster Computing, no. 23, pp. 1281-1291, 2020.
- [9] M. J. Z. H. V. M. and A. F. Eskandari "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices", IEEE Internet of Things Journal,, vol. 8, no. 7, pp. 6882-6897, 2020.
- [10] P. K. G. M. C. P. E. S. and G. P. Keserwani, "A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO-PSO-RF mode", Journal of Reliable Intelligent Environments, no. 7, pp. 3-21, 2021. .