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. Integrating SDN and NFV gives operators the flexibility and scalability they need to effectively enforce security rules in IoT environments.. Despite this background effort, many articles have explored models for implementing Security as a Service (SECaaS). Building a comparable approach leveraging SDN and NFV capabilities in the IoT networking arena has considerable support from both business and academics. On the other side, the rise in IoT assaults necessitates a modification that may stop unidentified attacks utilizing various detection techniques. IoT devices might have additional features and services added to them, 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 IoTThe 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 reauthenticating 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

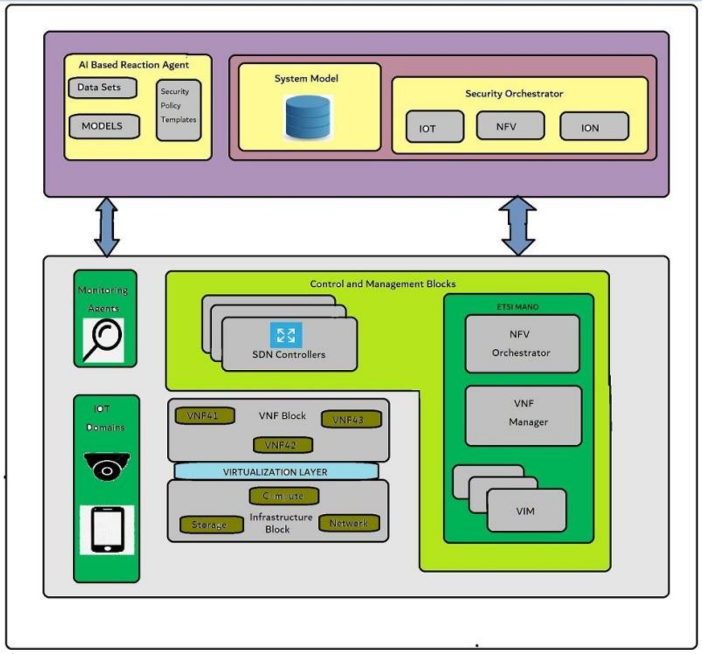

Fig. 1. Architecture of the Framework

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 protocol 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.

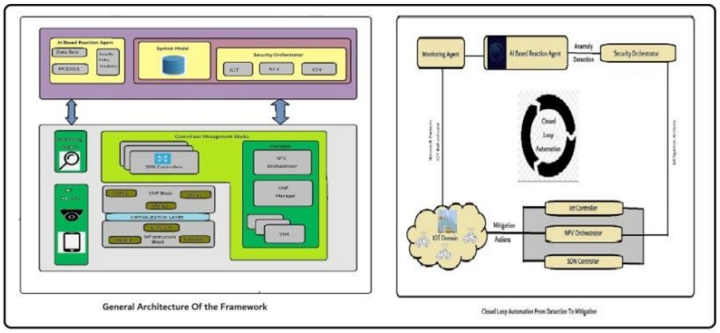

Fig. 2. Framework Overview

- 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).

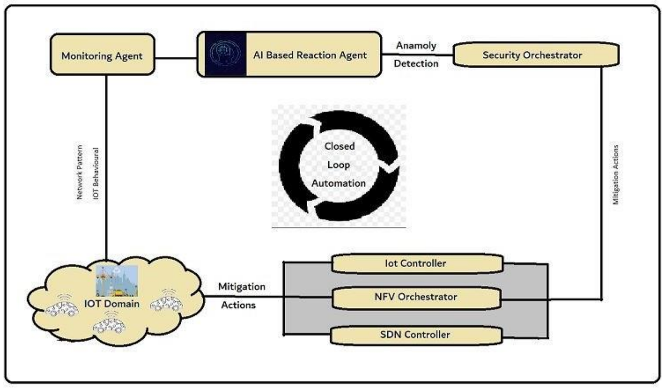

Fig. 3. Closed Loop Automation

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, Valves).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 liveProviding 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 Automotive 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. .