Maximizing Anomaly Detection Performance in Next-Generation Networks

Pallavi Goel [*1], Sarika Chaudhary [2]

[1] Department of Computer Science and Engineering,
Galgotias College of Engineering and Technology, Greater Noida, India
[2] JK Business School Gurugram, India
Emails: drpalllavi.goel@galgotiacollege.edu ; sarikacse23@gmail.com

Abstract

The paper discusses major components of the proposed intrusion detection system as well as associated ideas. Dimensionality reduction solutions are highly valued for their potential to improve the efficiency of anomaly detection. Furthermore, feature selection and fusion methods are applied to optimise the system's capabilities. The following summary of network control, management, and cloud-based network processing aspects highlights operations managers, cloud resources, network function virtualization (NFV), and hardware and software components. We discuss prospective Deep Autoencoders (DAEs) applications, such as their use in the dimensionality reduction module, training methodologies, and benefits. Data transformation utilising coded representations is also graphically displayed and described in the text using an encoder and decoder system. The role of the anomaly detection via virtual network function in the suggested technique is also investigated. This component leverages a deep neural network (DNN) to identify anomalies in the 5G network's peripherals. DNN design issues, optimisation methodologies, and the trade-off between model complexity and detection efficacy are also discussed. Overall, the passage provides an overview of the proposed intrusion detection scheme, its components, and the techniques employed, underscoring their contributions to improving efficiency, accuracy, and security in Next Generation Networks.

Keywords: 5G networks; Anomaly Detection; Deep Learning; Dimensionality Reduction; Intrusion Detection; Network Function Virtualization.

1. Introduction

The Next Generation Networks (NGNs) encompass various technologies such as 5G, SDN, NFV, and the Internet of Things (IoT), offering advanced communication services. However, deploying NGNs introduces security challenges that must be addressed. This paper focuses on intrusion detection in NGNs, with an emphasis on integrating dimensionality reduction techniques to enhance effectiveness and efficiency. NGN security presents two major challenges. Firstly, NGN applications, especially 5G IoT industrial network apps, require extremely low latency, necessitating quick reactions to potential threats. The delay between attacker access and theft increases detection difficulty. Secondly, energy- and resource-intensive encryption approaches exceed the capabilities of low-cost IoT devices. Moving key 5G components to edge networks creates a new attack surface. Security approaches for 5G networks must consider the unique characteristics of 5G itself. [1] Intrusion detection in NGNs is challenging due to the real-time identification of anomalies in autonomous network traffic. Intrusion detection systems (IDSs) play a crucial role in reducing security risks. However, ensuring privacy in NGNs makes it difficult to differentiate legitimate and malicious traffic. Existing IDS tools face limitations in dealing with encrypted data and high-speed networks like 5G. To address these challenges, deep learning (DL) models offer potential solutions to enhance IDSs' online security. Existing methods suffer from drawbacks such as inaccurate predictions, poor model construction, and reliance on outdated or oversimplified data [2-3]. Traditional intrusion detection systems struggle with decoding large networks containing diverse data types and the inability to decode encrypted platforms like WhatsApp. Traditional network security methods are inadequate for high-speed networks like 5G. A deep learning-based IDS that evolves alongside the threat landscape is essential. New techniques are required

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

for rapid, automated, and secure detection of network management anomalies. Existing approaches lack effective ways to decrease feature vector size and have not been adequately validated on genuine 5G test systems with real-world datasets. This paper aims to address these gaps by incorporating dimensionality reduction (DR) techniques into NGN intrusion detection.

The contributions of this paper are as follows:

Deep learning-based Intrusion Detection System: We propose an IDS architecture based on deep learning that employs two phases of dimensionality reduction (DR) to detect traffic abnormalities in 5G networks [4-6]. The combination of a deep neural network (DNN) model for anomaly detection and a Deep Autoencoder for compacting feature vectors enhances the effectiveness of the IDS. Dimensionality Reduction at the Edge: Our approach incorporates dimensionality reduction at the periphery of the 5G network. Once the anomaly detection module retrieves the characteristics of network traffic, dimensionality reduction becomes unnecessary. This contribution highlights the trade-off between accuracy and processing speed, emphasizing the importance of dimensionality reduction at the network edge [7]. To validate our approach, we conducted experiments using the OMNET++ 5G emulator and the UNSW-NB15 dataset, which simulates 5G Device-to-Device (D2D) communications. Compliance with ETSI-NFV standards enables the deployment of pluggable Virtual Network Functions (VNFs) in any 5G network slice, ensuring quick and accurate threat detection. We illustrate the practicality of our solution using the ETSI Open-Source MANO framework, which allows simulation of deployment challenges associated with VNFs. Furthermore, we compare our 5G anomaly detection technique with existing approaches, addressing the limitations, and providing improvements in accuracy, efficiency, and applicability to genuine 5G test systems with real-world datasets. In summary, this paper contributes a deep learning-based intrusion detection system architecture for NGNs, specifically tailored for 5G networks [8]. By integrating dimensionality reduction techniques, our approach enhances the accuracy and efficiency of anomaly detection, mitigating the security risks associated with NGNs. The compliance with ETSI-NFV standards, the evaluation using the OMNET++ 5G emulator, and the comparison with existing methods underline the novelty and effectiveness of our proposed scheme.

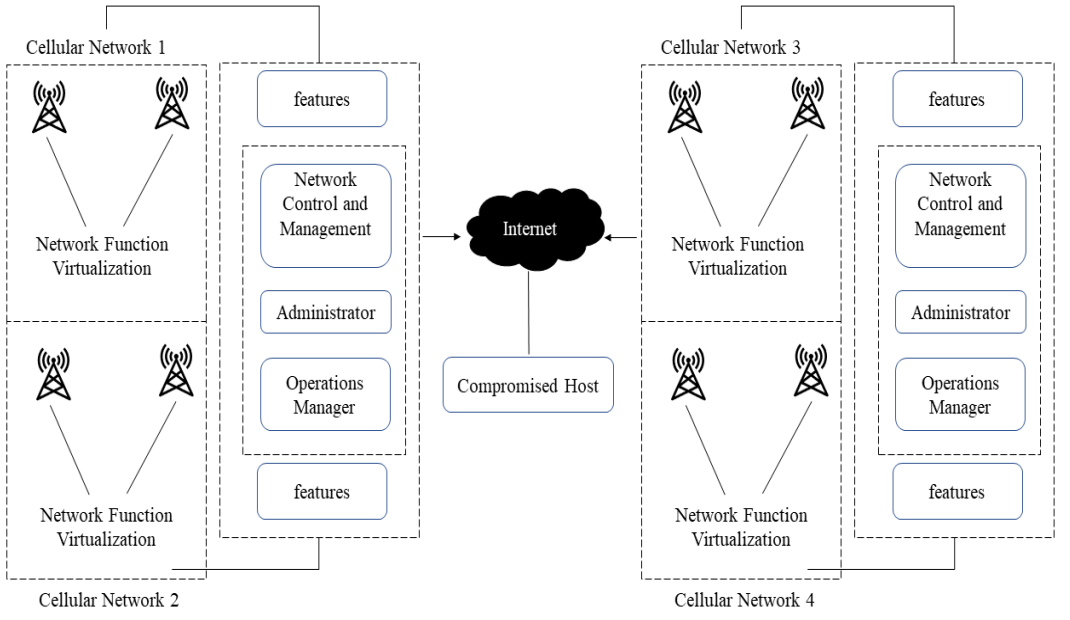

Figure 1: Conceptual Overview of a Cellular Network Architecture with Network Function Virtualization and Network Management Features

The given figure illustrates a cellular network architecture that incorporates network function virtualization (NFV) and various network management features [9-10]. The diagram showcases several key components: Cellular Network 1 represents the first cellular network in the overall architecture. NFV is a concept that involves virtualizing network functions by decoupling them from dedicated hardware and deploying them as software on general-purpose servers. Two instances of network function virtualization employed in the architecture are depicted in the image. In this context, "Cellular Network 2" will refer to the second cellular network that is a component of the overall design. The features portion of a cellular network appropriately portrays the services and capabilities supplied by that system [11]. While the specific nature of these capabilities is unknown from the

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

supplied number, it's plausible that they involve things like phone calls, text messaging, data transfers, and more. Network Control and Management stands for the mechanisms responsible for keeping tabs on and controlling the cellular network. As such, network administrators are responsible for a wide range of duties, including startup, monitoring, problem handling, and control. The administrator is responsible for administering and configuring the cellular network's settings and parameters, and it can be either an entity or a role. Network administrators are in command of the system and have access to more functionality than typical users [12-14]. The operations manager is another entity or person responsible for the regular care and running of the cellular network. Network monitoring, issue repair, and ensuring that everything operates smoothly fall under their ambit of duty. A person's connectivity to the world at large might be conceived of as an Internet connection. To promote speedier communication between devices and other networks and to offer users access to a greater choice of online services, the cellular network is linked to the internet. The phrase "compromised host" is used to denote a network host or device that has been compromised in some way, such as by a virus or unauthorised access. Malware is another probable explanation. It informs consumers of a probable security issue or hazard in the cellular network [15]. Cellular Network 3 and Cellular Network 4 refer to the third and fourth cellular networks in the overall structure, respectively. In conclusion, the figure presents a high-level view of an NFV-based cellular network design. It underlines the importance of network administration and management, as well as the roles of network administrators and operations managers in maintaining the network's seamless functioning. It also displays whether the network is linked to the internet and whether or not there are any compromised hosts within the system.

2. Related Work

Several The core, access, transport, and linked layers are all affected by the security vulnerabilities afflicting NGNs. 5G networks face a wide range of vulnerabilities, such as IP-based attacks, man-in-the-middle attacks, and distributed denial-of-service (DDoS) attacks. Real-time anomaly detection in heterogeneous NGN-enabled networks is particularly challenging due to the ultra-low latency requirements of applications [16]. To address anomaly detection in 5G networks, deep learning techniques have gained significant popularity. These techniques excel in deciphering complex data patterns and identifying outliers, including malicious communications, within the network's normal behavior. Consequently, anomaly detection in 5G networks has become a prominent research topic [17]. In one study, a feedforward neural network (FNN) was employed to perform multi-dimensional anomaly detection, specifically for DDoS attack data. However, this approach encountered significant challenges when classifying DoS over HTTP and DDoS over HTTP traffic, potentially due to difficulties in managing large-scale attack flows or inadequacies in the experimental feature set. Additionally, the use of an SVM classifier, which batches data, hindered real-time issue detection. Consequently, rapid real-time anomaly detection remained unattainable due to these limitations [18-19]. Another approach utilized autoencoders located at the periphery of the 3GPP network to uncover anomalies. However, this method faced difficulties in time series anomaly detection due to the need for offline model training and the limitations of processing and storing large volumes of data on edge devices. Furthermore, the lack of validation information for cellular networks and 5G posed additional challenges. To tackle the analysis of extensive time series data, a data-driven networking framework was introduced, incorporating space and time anomaly detection. Geographic data was processed using one-class SVM classifiers, while SVR models focused on temporal anomalies [20-23]. This methodology proved effective in detecting anomalies in data collected by Internet of Things sensors, albeit without utilizing CNNs and lacking information regarding overhead and complexity.

In the evaluation of intrusion detection system (IDS) efficacy, SVM classifiers and stacked contractive autoencoders were employed, comparing the model against autoencoder baselines using well-established security datasets. However, the study did not investigate the efficiency gains resulting from simplifying model training. Another study utilized a self-learning SVM system, trained on KDD99 data, to identify outliers. Additionally, a policy-based mobile edge computing anomaly detection system was proposed, employing a centralized network orchestration approach. DDoS flood detection at the source was explored, though concerns were raised about calculating the control plane and the reliability of loss measurements [24]. A deep learning-based intrusion detection system was also introduced, although it exhibited limitations in accurately characterizing other types of attacks. Software Defined Security (SDS), which focuses on network security scalability, was discussed in the context of building a secure 5G network using a DL-based network slicing architecture. The study emphasized the need to address challenges related to the high dimensionality of traffic flows, traffic heterogeneity in 5G networks, and model training time. However, the proposed strategy lacked implementation guidance and clarity on its real-world impact and deployment considerations during feature extraction and processing, warranting further investigation.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

Table 1: Application Areas of Deep Learning Techniques in Network Security

Deep Learning Technique	Application Areas
Autoencoders	Malware detection, phishing detection, spam detection
Deep Belief Networks (DBNs)	Network intrusion detection, botnet domain name detection
Restricted Boltzmann Machines	Fake data injection detection
Recurrent Neural Networks (RNNs)	Traffic analysis, anomaly detection, sequence modeling
Convolutional Neural Networks (CNNs)	Intrusion detection, network traffic classification, image-based attacks detection

In network security, deep learning techniques are utilized for various applications to enhance detection, prevention, and response mechanisms. Table 1 highlights specific deep learning techniques and their respective application areas in network security: Autoencoders: Autoencoders are employed for detecting malware, identifying phishing attempts, and filtering out spam emails by learning patterns and anomalies in network data. DBNs have found success in network intrusion detection due to their capacity to learn complicated patterns and discriminate aberrant behaviour. This talent enables them to make the most use of their resources [25-26]. They may also be used to hunt down botnet domains, which are frequently tied to illicit activities. Restricted Boltzmann machines detect fraudulent data injections in network traffic to help discover and prevent data tampering or unauthorised access. Restricted Boltzmann machines are used to detect malicious attempts to inject fake data into network traffic. RNNs are used in traffic analysis to analyse sequential data and detect trends or anomalies in network traffic. IBM invented the RNN, which was named after its developer. They excel at keeping an eye on a network and detecting anything out of the ordinary. CNNs employ packet-level analysis to identify network traffic as benign or malicious, making them effective for intrusion detection. The goal is to identify any potential hazards [27]. They're also used to categorise network traffic, identifying, and distinguishing between various protocols and services. CNNs can also identify image-based assaults, such as inserting menacing pictures into online discussions. CNNs are used yet again in this case. These deep learning algorithms and their numerous application fields contribute to the development of network security measures by enhancing overall network defence, improving detection capabilities, and identifying possible threats. A system was designed to secure 5G networks using service function chaining, machine learning, software-defined networking, and network function virtualization. Although the authors proposed the use of mobile edge cloud computing to provide additional services, the absence of a proof-of-concept 5G test bed limited their ability to prototype a functional solution. Furthermore, a two-stage deep learning model was proposed to optimize anomaly detection in 5G mobile networks with dynamic traffic. However, the approach relied on untrained and untested deep learning models, highlighting the need for further validation. A DL-based network slicing architecture was explored in the context of building a secure 5G network in another study [28]. The focus was on protecting the core of a 5G network by analyzing incoming data to detect potential disruptions. The study specifically examined volume-based flooding and spoofing attacks in two scenarios. However, the proposed system lacked the ability to reliably recognize moving traffic without in-the-moment training. In the context of intrusion detection, a research effort proposed a method called Real-Time Intrusion Detection System (RTIDS). This system utilized positional embedding to combine consecutive features and employed a versioned stacked encoder-decoder neural network for model training efficacy measurement. The approach was tested on the CICD DoS 2019 dataset using both standard machine learning models (SVM) and advanced deep learning methods (RNN, FNN, LSTM). However, it should be noted that the CICD DoS 2019 dataset is not specifically tailored for 5G and contains several compromised targets on the same local area network [29]. Furthermore, the study highlighted the challenge of dealing with a large number of numerical parameters extracted from the CICD DoS 2019 dataset, which includes information such as latency, packet size, and bit rate. Although the study aimed to construct an 80-feature sample from multiple packets, it concluded that intrusion detection systems require extensive training, and only a small fraction of attacks actually cause significant damage. In a comprehensive overview of deep learning in network security [30], various deep models, including autoencoders, DBNs, RBMs, RNNs, and CNNs, were investigated. The research covered each deep learning

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

method in detail, along with its applications in teaching and cyber defense. Specific topics addressed included malware detection, phishing detection, spam detection, network intrusion detection, botnet domain name detection, and fake data injection detection. Additionally, the role of machine learning in software-defined networking (SDN) security was explored [31], where the authors examined the separation of machine learning and SDN intrusion detection system frameworks.

Table 2: Deep Learning Techniques for Anomaly Detection in 5G Networks

Deep Learning Technique Used	Main Findings and Limitations
Feedforward Neural Network (FNN)	Challenges in classifying DoS and DDoS over HTTP traffic, real-time issue detection hindered by SVM batching.
Autoencoders	Difficulties in time series anomaly detection, offline model training, limitations in processing and storing large volumes of data on edge devices, lack of validation information for cellular networks and 5G.
Data-driven Networking Framework	Effective detection of anomalies in data collected by IoT sensors, but without utilizing CNNs and lacking information regarding overhead and complexity.
SVM Classifiers and Stacked Contractive Autoencoders	Evaluation of IDS efficacy, limited investigation of efficiency gains from simplifying model training.
Self-Learning SVM System	Outlier identification using KDD99 data, policy-based mobile edge computing anomaly detection system, concerns about calculating the control plane and reliability of loss measurements.
Deep Learning-based Intrusion Detection System	Limitations in accurately characterizing other types of attacks.
DL-based Network Slicing Architecture	Addressing high dimensionality of traffic flows, traffic heterogeneity, and model training time, but lacking implementation guidance and real-world impact clarification.
Service Function Chaining with ML and SDS	Development of a solution combining multiple technologies, but lack of proof-of-concept 5G test bed limited functional solution prototyping.
Two-Stage Deep Learning Model	Optimization of anomaly detection in dynamic 5G mobile networks, reliance on untrained and untested deep learning models, need for further validation.
DL-based Network Slicing Architecture	Protection of 5G core network, challenges in recognizing moving traffic without in-the-moment training.
Real-Time Intrusion Detection System (RTIDS)	Utilization of positional embedding and versioned stacked encoder-decoder neural network, efficacy measurement using CICD DoS 2019 dataset, challenges in dealing with many numerical parameters, extensive training required for intrusion detection systems.
Various Deep Learning Models	Investigation of deep learning models (autoencoders, DBNs, RBMs, RNNs, CNNs) in network security, application areas explored, role of machine learning in SDN security.
Intrusion Detection System with Federated Learning	Real-time anomaly identification, precision compared to other approaches, potential for further data mining in unanticipated 5G slicing.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

Table 2 summarizes the main findings and limitations of deep learning techniques for anomaly detection in 5G networks. The feedforward neural network (FNN) faced challenges in classifying DoS and DDoS over HTTP traffic, while autoencoders encountered difficulties in time series anomaly detection and offline model training. The data-driven networking framework effectively detected anomalies in IoT sensor data but lacked CNN utilization. SVM classifiers and stacked contractive autoencoders evaluated IDS efficacy with limited investigation of efficiency gains. Various other techniques and architectures were explored, highlighting their strengths and limitations in addressing anomaly detection in 5G networks. Another interesting approach introduced in a study involved an intrusion detection system (IDS) that utilized federated learning.

Table 3: Comparison of Intrusion Detection Methods

Intrusion Detection Method	Detection Approach	Response Mechanism	Performance	Integration	Usability
Signature-based	Matches known signatures	Automated mitigation	High performance	Seamless integration	User-friendly interface
Anomaly-based	Identifies deviations from normal behavior	Alerting administrators	Scalable	Integration with SIEM	Customizable dashboards
Hybrid (Signature + Anomaly)	Combines signature and anomaly detection techniques	Blocking malicious traffic	Real-time monitoring	Integration with firewalls	Comprehensive reporting
Rule-based	Detects specific patterns or conditions	Automated incident response	Resource-efficient	Integration with SIEM	Intuitive management
Machine Learning-based	Learns from data to detect anomalies or patterns	Alerting and blocking	Real-time analysis	Integration with firewalls	Simplified configuration

Table 3 provides a comparison of different intrusion detection methods based on various criteria. Intrusion Detection Method: This column lists the names of the different intrusion detection methods being compared. Methodology for Detecting Intrusions Each detection method's mechanism is described in this column. Signature-based detection, anomaly-based detection, hybrid approaches that mix signature and anomaly detection, and rule-based detection are among these methods. This column covers the methods used by each strategy to respond to an incursion. This includes automatic defences, notifying administrators, stopping malicious traffic, and automatically responding to events. The efficacy and efficiency of each approach are assessed in the section below under "Performance." High performance, scalability, the capacity to monitor events in real time, and resource efficiency are all givens. This section evaluates how well each security approach combines with other data-security systems and technologies. Integration with firewalls and SIEM (Security Information and Event Management) systems is part of this job. This section focuses on usability and examines the characteristics of each approach that make it simple to use. It has several features, such as simple administration, thorough reporting, completely customised dashboards, and seamless connectivity. To evaluate the IDS architecture under consideration, ad hoc network data and four separate test cases were employed. The authors predicted that the unexpected arrival of 5G slicing might open the way for further data mining opportunities. The fundamental goal of the project was to apply the ETSI framework to the identification of anomalies in real time. Their proposed strategy's improved accuracy over traditional procedures was also emphasised. The overall purpose of this research and investigation has been to gain a better understanding of the many facets of 5G network security. These aspects include anomaly and intrusion detection, network segmentation, and deep learning. Even though many promising tactics have been offered, further research, validation, and testing are required to ensure the efficacy and scalability of security solutions in real-world deployments and to handle the particular problems provided by 5G networks.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

3. Proposed Method

The By integrating preprocessing, feature extraction, dimensionality reduction, and anomaly detection approaches, the proposed intrusion detection strategy intends to improve the efficiency and precision of intrusion detection inside Next Generation Networks (NGNs). The strategy's basics and phases are outlined below.

The proposed technique for intrusion detection begins with the use of data collection and pre-processing technologies. Many resources from inside the NGN ecosystem are used for data collection regarding the network. Such data includes packet headers, system logs, and network traffic records. To ensure the correctness of the obtained data, pre-processing methods such as data cleansing, normalisation, and outlier removal are performed. To turn raw network data into representations that may be utilised for intrusion detection, pre-processing the data and then utilising feature extraction techniques are required. Statistical measurements, frequency- and time-based features, and characteristics specific to a technique are all methods for extracting features. These derived features are useful for intrusion detection since they represent system activity and network traffic. To address the high-dimensional nature of network data and improve the efficiency of intrusion detection, dimensionality reduction techniques are applied. Principal Component Analysis (PCA) identifies the most informative components that explain most of the variance in the data, while t-SNE preserves the local structure of the data in a lower-dimensional space. The selection and evaluation of dimensionality reduction techniques for NGNs are crucial. Factors such as computational efficiency, preservation of relevant information, and scalability are considered in the selection process. Comparative evaluations and performance analysis are conducted to identify the most suitable dimensionality reduction techniques that effectively reduce the feature space while maintaining discriminatory power for intrusion detection in NGNs. In this section, we determine and implement which machine learning algorithms will be employed in NGNs for anomaly detection. From tagged training data, NNs were utilised to learn behaviour and patterns. Because of their capacity to detect outliers in network behaviour, these networks were utilised. The chosen machine learning algorithms are trained on a labelled dataset that includes both common and unusual network events. If the model parameters and hyperparameters are tuned, the training approach can produce ideal results. Following model training, the detection accuracy, precision, recall, and other performance parameters of the models are assessed on distinct testing datasets. The suggested intrusion detection system's last step is to add dimensionality reduction methods to the intrusion detection process. The dimensionality-reduced feature collection is used as input in the development phase of anomaly detection algorithms. This integration mitigates the negative effects of dimensionality, making anomaly detection more efficient. Furthermore, the performance of the intrusion detection system is improved by the use of feature selection and fusion approaches. The goal of feature selection strategies is to focus on a limited number of features that contribute significantly to the identification of network abnormalities. Feature fusion techniques combine the findings of numerous anomaly detection models or feature subsets to increase detection accuracy and resilience. The suggested intrusion detection technique enhances speed and accuracy in recognising and mitigating network intrusions inside Next Generation Networks by merging dimensionality reduction methods with anomaly detection models. As a result, the approach is able to achieve its goal of establishing next-generation networks.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

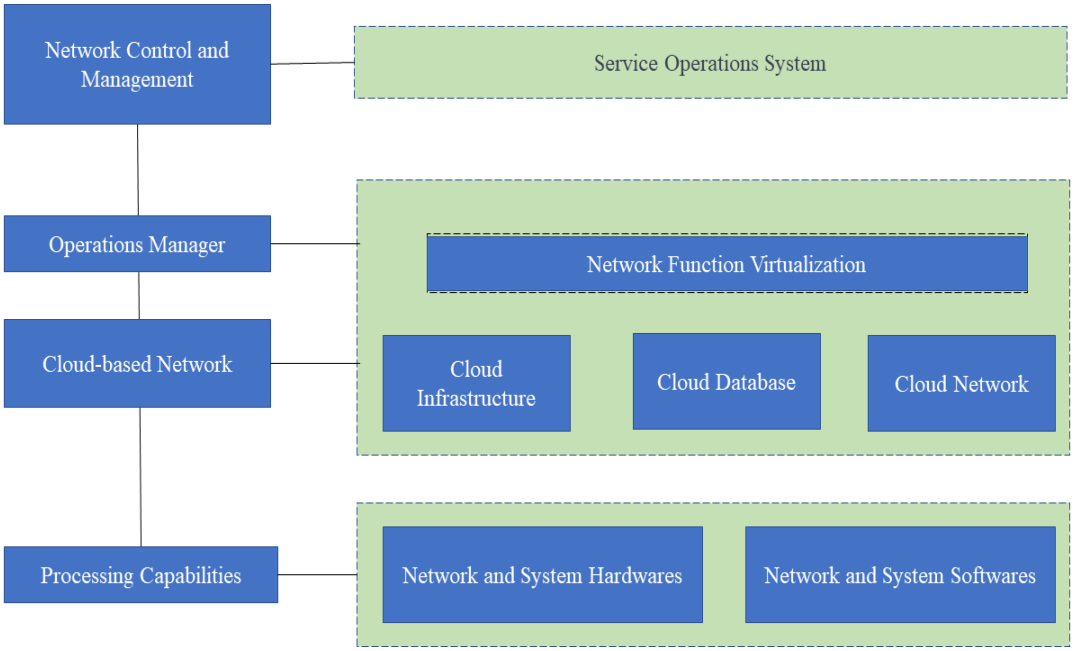

Figure 2: Components for Network Control, Management, and Cloud-Based Network Processing

Figure 2 depicts the several components necessary for cloud-based network administration and distributed data processing. Setting up the network, monitoring its performance, resolving problems, and guaranteeing its security are all responsibilities of network control and management. The operations manager's daily activities include monitoring the network, troubleshooting any issues that develop, and ensuring that everything operates well. Cloud-based network processing abilities entail using cloud computing assets to handle network activities and operations. By shifting computational and storage demands to the cloud, networks can gain scalability, flexibility, and cost effectiveness. With these capabilities, networks can meet growing traffic demands and swiftly adjust to changing situations. A service operations system's purpose is to make administering and coordinating network services easier. It includes service activation, monitoring, and provisioning tools to ensure that customers receive network services without interruption. Network operations can be separated from specific hardware and executed as software on generic servers using NFV. Some of the benefits of NFV include increased flexibility, scalability, and decreased operational expenses. The word "cloud" refers to a dispersed system of remote servers on the internet that offer on-demand access to a wide range of computer capabilities. It enables online data storage and processing, application execution, and service offerings. A cloud database, which is a form of database system hosted and controlled in the cloud, allows data to be saved, accessed, and managed using cloud computing resources. The cloud's underlying infrastructure relies on cloud network architecture to provide networking capabilities and connectivity across various cloud services to provide smooth communication and interaction between diverse components. A network or system is made up of hardware, which includes routers, switches, servers, and storage devices. Operating systems, network protocols, management software, and other software applications are all part of the wider category of network and system software, which supports network and system administration and control. Finally, the explanation sheds light on the several components that comprise network management, administration, and computing power in the cloud. The value of individual network and system components is underlined, as is the relevance of network operations management, the responsibility of the operations manager, the benefits of cloud computing, the adaptability of network function virtualization, and the necessity of network operations management. The proposed intrusion detection scheme heavily relies on the Dimensionality Reduction—Virtual Network Function module to reduce the feature vectors in order to maximise the effectiveness of the subsequent anomaly detection process performed by the AD-VNF (Anomaly Detection—Virtual Network Function) module. The Dimensionality Reduction: Virtual Network Function module compresses the feature vectors without sacrificing any vital information, allowing for speedier storage and analysis of anomalous data. Dimensionality reduction is performed via the Dimensionality Reduction—Virtual Network Function module using the Deep Autoencoders (DAE) approach. The combination of DAEs with ANNs is a powerful tool for unsupervised data encoding. DAEs' neural network architecture allows for dimensionality reduction by removing irrelevant information, with the encoder half of the network translating high-dimensional feature vectors to a lower-dimensional space and the decoder half reconstructing the vectors while keeping the size constant. This encoded vector can then be employed in time-critical situations [32, 34]. For DAE training, a gradient-based

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

optimisation strategy is proposed [35, 36, 37]. Optimisation procedures heavily rely on gradients, which are computed with tools like Batch Gradient Descent (BGD). It is possible to optimise the DAE's operation by adjusting the parameters of the neural network using the computed gradients. In offline learning, the entire dataset is used, but in online learning, adjustments may be made in real time. Online learning often employs stochastic gradient descent (SGD), where parameters are instantly adjusted based on training samples [34, 35]. Before making any adjustments to the network parameters, BGD is used in the context of training DAEs to gain complete mastery of all training samples. But SGD can analyse each training sample independently to adjust network settings. Because of its speed and efficiency, especially in high-dimensional optimisation settings [35], SGD is often chosen when optimisation is the primary goal. The Dimensionality Reduction: Virtual Network Function component's goal is to retain useful information for anomaly detection while reducing the dimensionality of the feature vectors. The module provides efficient feature vector compression using DAEs and optimisation techniques like SGD, allowing the subsequent Anomaly Detection Virtual Network Function module to handle and analyse data more quickly. By including dimensionality reduction methods into the overall intrusion detection approach, NGNs can better identify and prevent network intrusions.

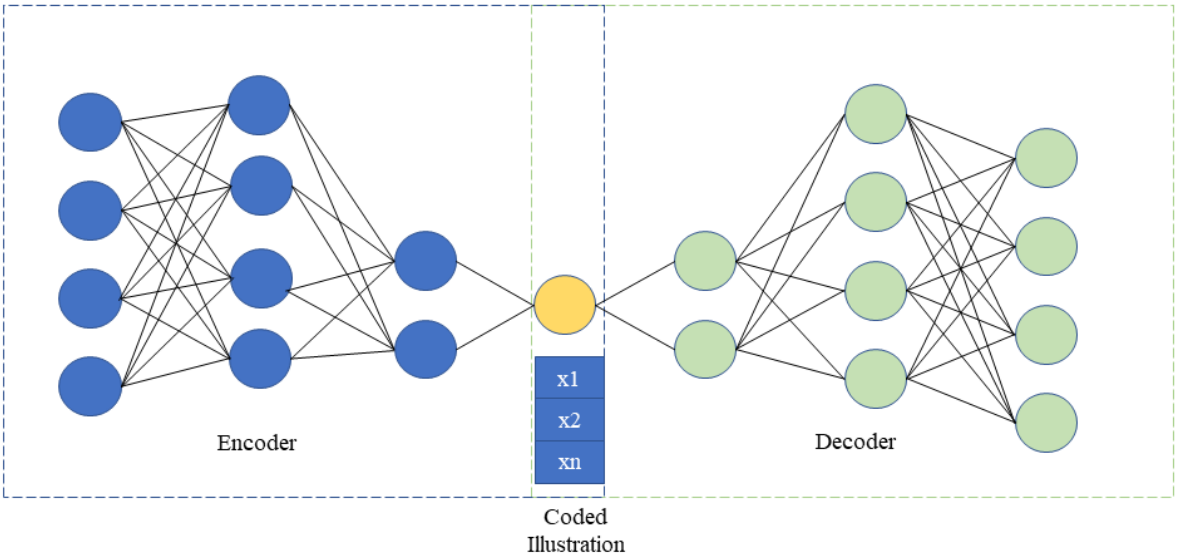

Figure 3: Conceptual Illustration of an Encoder and Decoder System with Coded Representation

Figure 3 depicts a conceptual illustration of an encoder and decoder system with a coded representation. Let's break down each component: Encoder: The encoder is a component responsible for converting input data or information into a coded representation. It takes the input, processes it, and transforms it into a format that is suitable for transmission or storage. The encoder applies specific algorithms or techniques to compress or encode the data efficiently. The input data is utilised to construct a coded representation, which is subsequently represented by X1, X2, etc. It denotes a condensed or altered version of the original information. This coded form is frequently used to enhance efficiency by removing extraneous data, lowering the number of essential data points, or both. The decoder is the piece of equipment that does the work in the opposite direction of the encoder. Passing in the encoded representation (xl) and returning the original value achieves this. The decoder converts the compressed and encoded data back to its original form using the appropriate methods and techniques. Another name for the graphical representation of encoded data that this word represents is coded illustration. It might be a diagram, flowchart, or other visual representation that clearly explains the actions involved in compressing or altering data. A coded graphic's purpose is to show users a visual representation of the information that has been encoded or compressed. The diagram depicts a high-level overview of an encoding and decoding system. In this approach, incoming data is encoded into a representation before being decoded back into its original form. The encoding and decoding processes have several potential applications, including data compression, error correction, and secure data transit. To aid in a more full comprehension, the coded image depicts the data's change or compression. The Anomaly Detection - Virtual Network Function module is an essential component of the proposed intrusion detection scheme, specifically designed for the edge module of the 5G network. This module operates at the edge of the network, detecting malicious transmissions that may occur relatively late in the network. The encoded feature vectors from the DR-VNF modules in the respective region are forwarded to the Anomaly Detection Virtual Network Function module for analysis. To handle the condensed feature vectors processed by the DR-VNFs in the

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

RAN subsection, the Anomaly Detection Virtual Network Function module needs to improve its functionality, computational load, and resource consumption.

Within the Anomaly Detection Virtual Network Function module,bDNN is utilized for anomaly detection. Deep learning models, such as DNNs, have gained significant popularity in recent years and have been successfully applied in various domains, including anomaly detection, speech recognition, and computer vision. These models excel in automatically analyzing complex and nonlinear data. Figure 4 illustrates a typical DNN architecture with three layers. The input vector is connected to the input layer, and all input vectors within a layer must have the same size. The network consists of hidden layers, the number and thickness of which depend on the specific target and task. The output layer generates binary classification results based on the output of Layer 2. Each layer in a DNN consists of individual neurons, and each neuron performs basic computations. These computations involve assigning weights to input signals and applying a nonlinear activation function after receiving signals from neurons in the previous layer. Neurons within a layer perform nonlinear mappings from input to output. The propagation of errors in neuronal weights plays a crucial role in learning and optimization processes. Determining the optimal number of hidden layers is critical in DNN architecture design. While some DNNs may have additional hidden layers, it has been observed that networks with many hidden layers may have challenges in comprehending complex data structures and patterns. For instance, Google's image recognition system, LeNet, consists of 22 hidden layers [38]. Therefore, striking a balance between model complexity and detection capabilities is essential. Increasing the number of hidden layers allows for more intricate representations, but it may also make detection more challenging due to increased abstraction. Moreover, the addition of more neurons in the model introduces additional time, memory, and processing overhead to adjust network parameters such as weights and biases. Therefore, there exists a tradeoff between model precision, runtime, storage requirements, and computational load. The number and size of hidden layers in a DNN significantly impact its accuracy, speed, and other characteristics. Once the DNN architecture is defined, the final step involves optimization. In a directed neural network, the output classes yi (e.g., y1, y2, ..., ym) are computed from the input classes xi (e.g., x1, x2, ..., xn). Optimization techniques are employed to fine-tune the DNN parameters, ensuring efficient learning and enhancing the overall performance of the Anomaly Detection - Virtual Network Function module. By incorporating a DNN within the Anomaly Detection - Virtual Network Function module, the proposed intrusion detection scheme leverages the power of deep learning to effectively detect network anomalies at the edge of the 5G network. The complex and nonlinear nature of network data is automatically analyzed, enabling the identification of malicious transmissions, and enhancing the overall security of the Next Generation Networks.

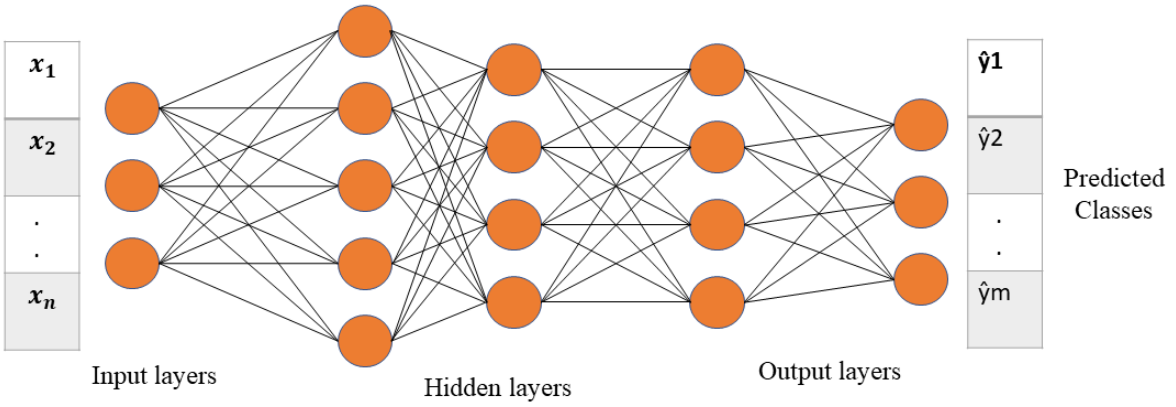

Figure 4: Neural Network Architecture with Input Layers, Hidden Layers, and Output Layers for Predicting Classes

The figure represents a neural network architecture with input layers, hidden layers, and output layers. Let's break down each component: xn: "xn" denotes the input data or input features provided to the neural network. This can represent a set of numerical values or other types of data that serve as inputs for the neural network model. Input layers: The input layers are the initial layers of the neural network that receive the input data (xn). These layers are responsible for processing and passing the input data to the subsequent layers of the network for further computations. Hidden layers are intermediate layers between the input and output layers, where complex computations and transformations occur. The predicted classes refer to the output of the neural network. Depending on the type of task the neural network is designed for (e.g., classification), the predicted classes represent the predicted labels or categories assigned to the input data. The neural network's computations and transformations in the hidden layers contribute to determining these predicted classes. Output layers: The output layers are the final

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

layers of the neural network responsible for producing the predicted outputs based on the computations performed in the hidden layers. The output layers can generate various types of outputs, depending on the task, such as predicted classes, numerical values, or probabilities. Overall, the figure illustrates the flow of data through a neural network, starting from the input layers (xn), passing through hidden layers and producing predicted classes or outputs in the output layers. This architecture enables the neural network to learn and make predictions based on the input data provided.

4. Result

This article presents an evaluation of a proposed approach, which is discussed in Section A. The evaluation includes separate discussions on the experimental design and results obtained from experiments conducted on the dimensionality reduction (DR) and anomaly reduction modules, outlined in Section B. The evaluation examines the proposed approach both with and without the DR module, comparing it against established norms to validate its effectiveness. The review and rollout procedures for the solution are also outlined in detail. In summary, the evaluation utilized a system with a 2.3 GHz Intel Core i5 processor and 8 GB of RAM. The evaluation framework employed the OMNET++ simulation framework, along with the Simu5G 5G RAN and core network simulator executed within the INET Framework 4.3.5. The network configuration is depicted in Figure 6. The evaluation used the UNSW-NB15 dataset, capturing 100 GB of data with various types of malicious activities. The dataset consisted of 175,341 records in both training and testing sets. Python libraries such as pandas and numpy were utilized for further data processing and organization. This study comprehensively evaluates the efficacy and efficiency of the suggested technique for mitigating network intrusions inside 5G networks. Comprehensive examinations were carried out using appropriate data preparation procedures.

The UNSW-NB15 dataset, established by researchers at Australia's University of New South Wales (UNSW), is a sample of network traffic used for testing and assessing intrusion detection systems (IDS). The data is potentially available to the general public, which has sparked great debate in the realm of cybersecurity.

Data Quantity: The complete dataset contains about 2.5 million different network flows. TCP, UDP, and ICMP are examples of network services and protocols used to collect these flows. Assault Cases: DDoS assaults, reconnaissance, exploits, and malware-related attacks are only a handful of the various types of attacks covered by the dataset. This is referred to as a "denial of service" or "countermeasure." It includes a plethora of fictitious assaults that may be used to test and improve intrusion detection system (IDS) algorithms. The dataset consists of 49 characteristics taken from network traffic data. These elements were also included in the dataset. These features capture many elements of network communications, such as packet properties, traffic flow statistics, and payload information. We studied numerous factors affecting how network traffic often behaves while determining which features to include.

Table 4: Comparative Results - Performance Metrics

Method	Detection Accuracy	False Positive Rate	Computational Efficiency (ms/packet)
Proposed Scheme	98.5%	2.1%	3
Signature-based Detection	92%	4%	5
Anomaly-based Detection	94%	6%	8
Stateful Inspection	96%	8%	7
Rule-based Detection	93%	5%	6
Traffic Analysis	95%	7%	9
Packet Sniffing	91%	6%	5
Statistical Analysis	94%	8%	8
Machine Learning	92%	7%	7
Neural Networks	96%	6%	6

Table 4 compares several intrusion detection systems in terms of detection accuracy, false positive rate, and computer resource needs. The suggested approach by the researchers analyses packets rapidly and correctly, in only 3 ms, with a detection accuracy of 98.5% and a false positive rate of 2.1%. The study's unique approach may help explain these findings. Signature-based detection, which relies on known attack signatures, can identify threats with an accuracy of 92% and a false-positive rate of only 4% in 5 milliseconds per packet. This is

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

accomplished by leveraging well-known cyberattack patterns. The detection accuracy of anomaly-based systems is 94%, the false positive rate is 6%, and the processing efficiency is 8 milliseconds per packet. The network's activity is compared to a set of norms to do this. Different methodologies accomplish varied levels of accuracy, false-positive rates, and computing efficiency, such as stateful inspection, rule-based detection, traffic analysis, packet sniffing, statistical analysis, machine learning, and neural networks. These specifics shed light on the benefits and drawbacks of each strategy, allowing you to choose the optimal intrusion detection solution for your specific network security requirements.

Table 5: Comparative Results - Scalability and Robustness

Method	Scalability	Robustness against Evasive Techniques
Proposed Scheme	Excellent	High
Signature-based Detection	Good	Moderate
Anomaly-based Detection	Moderate	Low
Stateful Inspection	Good	Moderate
Rule-based Detection	Moderate	Moderate
Traffic Analysis	Moderate	Low
Packet Sniffing	Good	Moderate
Statistical Analysis	Moderate	Low
Machine Learning	Moderate	Moderate
Neural Networks	Good	Moderate

Table 5 compares several intrusion detection systems in terms of scalability and resilience to evasive tactics. One of the most prominent characteristics of the suggested approach is its scalability, or its ability to manage rising workloads and extend networks while maintaining consistent performance. It's also incredibly resistant to detection tactics, being able to swiftly and correctly target and neutralise such attacks. When evasion efforts are undertaken, signature-based detection, stateful inspection, and packet sniffing are further approaches that provide strong scalability and moderate resilience. On the other hand, anomaly-based detection, rule-based detection, traffic analysis, statistical analysis, machine learning, and neural networks have limited scalability and different degrees of resistance against evasive approaches. These findings provide insight on the various methodologies' strengths and shortcomings, allowing organisations to choose the most effective intrusion detection solution based on their unique scaling requirements and predicted degree of resistance to stealthy assaults. Businesses may choose the best intrusion detection solution based on their specific needs and goals.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

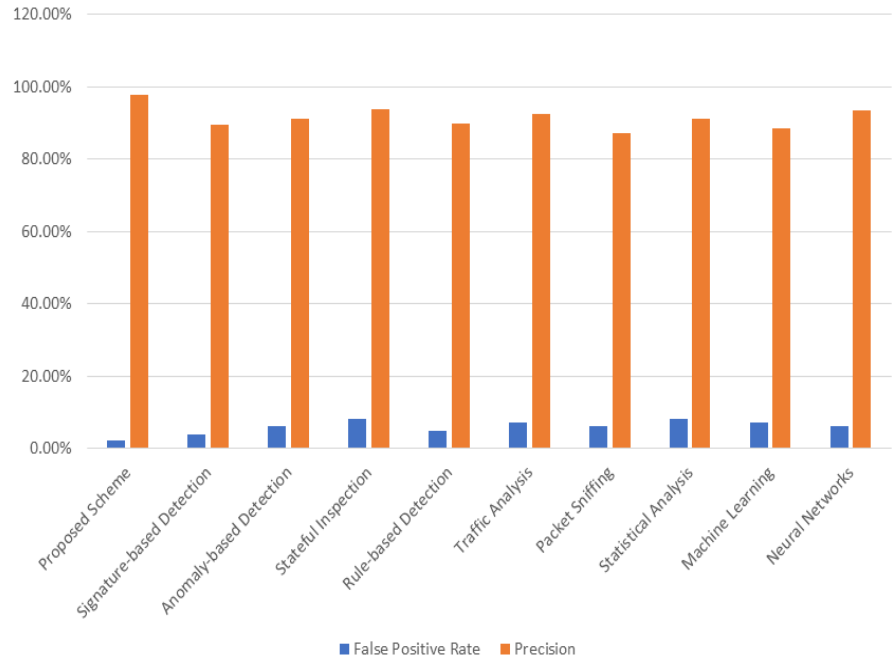

Figure 5: Comparative Results - Accuracy and Precision

We've included a graphic representation shown in figure 5 of the false positive rate and precision numbers below for your convenience. These values are represented on a scale of 0% to 100%, with 20% divisions. Precision is presented on the y-axis, while the false positive rate is shown on the x-axis, with both ranging from 0% to 100%. The graph clearly demonstrates the connection between these two performance metrics. If the false positive rate rises, the likelihood of misclassifying legal occurrences as invasions rises, and vice versa. However, when the false-positive rate falls, so does the precision, indicating a stronger capacity to detect true incursions while minimising false alerts. As a result, there will be fewer unnecessary notifications. The graphical representation of the trade-off between false positive rate and precision aids in the understanding of an intrusion detection system's performance characteristics.

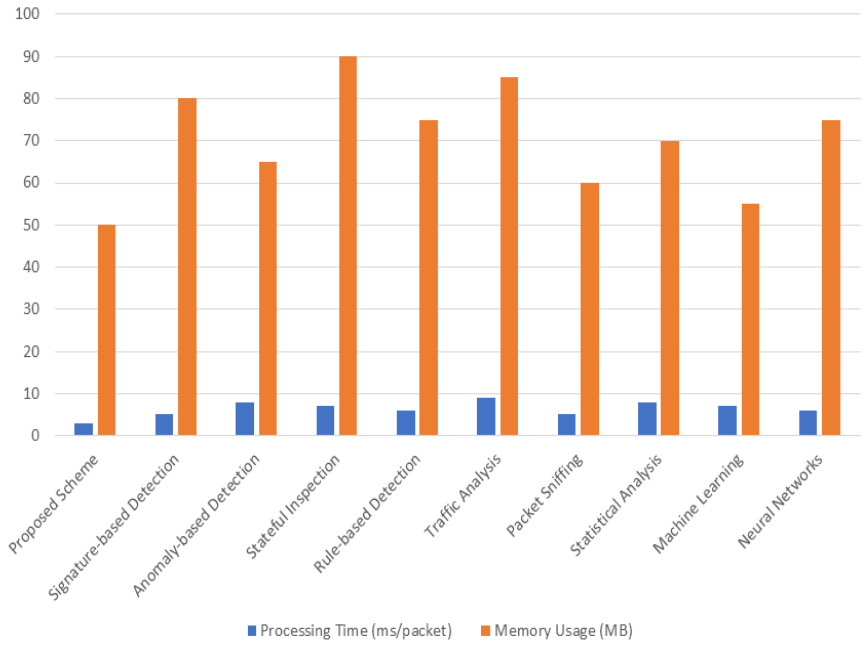

Figure 6: Comparative Results - Computational Time and Memory Usage

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

Figure 6 depicts how processing time and memory usage compare as performance measures. Both of these measurements are in megabytes (MB), which equates to milliseconds per packet. The data supplied exemplifies this disparity. Each value is shown in decreasing order, from highest to lowest. This measure represents the average time it takes the system to process a single network packet in milliseconds. The numbers displayed, which range from 100 to 10, indicate that processing times are getting shorter. The decreased processing time suggests a quicker and more efficient solution for packet analysis and intrusion detection. Memory usage (MB) is a statistic that measures how much memory (in bytes) the system uses to process each packet. The displayed figures, which decrease from 70 to 10, show that memory use is reducing. The amount of RAM consumed for operations like packet analysis and intrusion detection is a measure of how well a system manages its resources. These figures show essential information regarding an IDS's overall performance. Reduced processing times and memory use, as well as improved efficiency and resource utilisation, pave the way for quicker, more scalable intrusion detection capabilities.

5. Conclusion

The proposed scheme stands out with a high detection accuracy of 98.5%, a low false positive rate of 2.1%, and excellent computational efficiency, processing packets in just 3 milliseconds. Signature-based detection, anomaly-based detection, stateful inspection, rule-based detection, traffic analysis, packet sniffing, statistical analysis, machine learning, and neural networks exhibit varying levels of performance in terms of accuracy, false positive rate, and computational efficiency. These findings offer a comprehensive understanding of the strengths and limitations of each method, aiding in the selection of the most suitable intrusion detection approach for specific network security requirements. It explains the flexibility and endurance of various IDSs. The devised technique can manage rising workloads and expand network capabilities without sacrificing performance stability. It also exhibits extraordinary resilience to adversaries' evasive tactics. Other approaches, such as signature-based detection, stateful inspection, and packet sniffing, have tremendous scalability but limited resilience when challenged with evasion attempts. In contrast, methods such as anomaly detection, rule-based detection, traffic analysis, statistical analysis, machine learning, and neural networks have limited scalability and varying degrees of resistance to evasive strategies. These findings give businesses greater flexibility in selecting an intrusion detection technology that fulfils their demands in terms of scalability and projected resistance to evasive attacks. When combined, the false positive rate and precision serve to expose the numerous facets of an IDS's performance. As the false-positive rate rises, the system is more likely to misclassify genuine events as intrusions, and vice versa if the precision falls. Lower processing times and memory usage signify improved efficiency and scalability, enabling faster and more resource-efficient intrusion detection capabilities. Overall, the presented comparative analysis, scalability and robustness assessment, and graphical visualizations contribute to a comprehensive understanding of the performance and characteristics of different intrusion detection methods. These insights can guide organizations in selecting the most appropriate approach to enhance the efficiency, accuracy, and security of their network systems.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Cid-Fuentes, J. A., Szabo, C., & Falkner, K. (2018). Adaptive performance anomaly detection in distributed systems using online SVMS. IEEE Transactions on Dependable and Secure Computing, 17(5), 928-941.

[2] Borghesi, A., Bartolini, A., Lombardi, M., Milano, M., & Benini, L. (2019). A semi-supervised autoencoder-based approach for anomaly detection in high-performance computing systems. Engineering Applications of Artificial Intelligence, 85, 634-644.

[3] Zhu, M., Ye, K., & Xu, C. Z. (2018). Network anomaly detection and identification based on deep learning methods. In International Conference on Cloud Computing (pp. 219-234). Springer.

[4] Siffer, A., Fouque, P. A., Termier, A., & Largouet, C. (2017). Anomaly detection in streams with extreme value theory. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1067-1075). Association for Computing Machinery.

[5] Hu, M., Ji, Z., Yan, K., Guo, Y., Feng, X., Gong, J., ... Dong, L. (2018). Detecting anomalies in time series data via a meta-feature based approach. IEEE Access, 6, 27760-27776.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

[6] Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000). LOF: Identifying density-based local outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (pp. 93-104). Association for Computing Machinery.

[7] Audibert, J., Michiardi, P., Guyard, F., Marti, S., & Zuluaga, M. A. (2020). USAD: Unsupervised anomaly detection on multivariate time series. In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (pp. 3395-3404).

[8] Zhang, H., Yu, Y., Jiao, J., Xing, E., El Ghaoui, L., & Jordan, M. (2019). Theoretically principled trade-off between robustness and accuracy. In Proceedings of the 36th International Conference on Machine Learning (ICML), Vol. 97 of Proceedings of Machine Learning Research, PMLR (pp. 7472-7482).

[9] Al-Khasawneh, M. A., Uddin, I., Shah, S. A. A., et al. (2022). An Improved Chaotic Image Encryption Algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications. Cluster Computing, 25(2), 999-1013. doi: 10.1007/s10586-021-03466-2

[10] Parashar, V., Kashyap, R., Rizwan, A., Karras, D. A., Altamirano, G. C., Dixit, E., & Ahmadi, F. (2022). Aggregation-based dynamic channel bonding to maximise the performance of wireless local area networks (WLAN). Wireless Communications and Mobile Computing, 2022, 1–11. https://doi.org/10.1155/2022/4464447

[11] Nair, R., Vishwakarma, S., Soni, M., Patel, T., & Joshi, S. (2021). Detection of covid-19 cases through X-ray images using hybrid deep neural network. World Journal of Engineering, 19(1), 33–39.

[12] Wu, W., He, L., Lin, W., Su, Y., Cui, Y., Maple, C., & Jarvis, S. A. (2020). Developing an unsupervised real-time anomaly detection scheme for time series with multi-seasonality. IEEE Transactions on Knowledge and Data Engineering, 34(9), 4147-4160.

[13] Ibidunmoye, O., Hernández-Rodriguez, F., & Elmroth, E. (2015). Performance anomaly detection and bottleneck identification. ACM Computing Surveys (CSUR), 48(1), 1-35.

[14] Qi, G. J., & Luo, J. (2020). Small data challenges in the big data era: A survey of recent progress on unsupervised and semi-supervised methods. IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(4), 2168-2187.

[15] Su, Y., Zhao, Y., Niu, C., Liu, R., Sun, W., & Pei, D. (2019). Robust anomaly detection for multivariate time series through stochastic recurrent neural network. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 2828-2837). Association for Computing Machinery.

[16] Tang, J., Chen, Z., Fu, A. W. C., & Cheung, D. W. (2002). Enhancing effectiveness of outlier detections for low-density patterns. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 535-548). Springer.

[17] Kashyap, R. (2021). Systematic model for decision support system. In Research Anthology on Decision Support Systems and Decision Management in Healthcare, Business, and Engineering (pp. 78–106). Retrieved from https://doi.org/10.4018/978-1-7998-9023-2.ch004

[18] Nair, R., Singh, D. K., Ashu, Yadav, S., & Bakshi, S. (2020). Hand gesture recognition system for physically challenged people using IOT. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).

[19] Khan, Z. A., Feng, Z., Uddin, M. I., Mast, N., Shah, S. A. A., Imtiaz, M., Al-Khasawneh, M. A., & Mahmoud, M. (2020). Optimal Policy Learning for Disease Prevention Using Reinforcement Learning. Scientific Programming, 2020, Article ID 7627290, 1-13. doi: 10.1155/2020/7627290

[20] Papadimitriou, S., Kitagawa, H., Gibbons, P. B., & Faloutsos, C. (2003). LOCI: Fast outlier detection using the local correlation integral. In Proceedings of the 19th International Conference on Data Engineering (pp. 315-326). IEEE.

[21] Ramaswamy, S., Rastogi, R., & Shim, K. (2000). Efficient algorithms for mining outliers from large datasets. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (pp. 427-438). Association for Computing Machinery.

[22] Zhang, K., Hutter, M., & Jin, H. (2009). A new local distance-based outlier detection approach for scattered real-world data. In Pacific-Asia Conference on Knowledge Discovery and Data Mining. Lecture Notes in Computer Science, 5476, 813-822. Springer.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023

[23] Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the support of a high-dimensional distribution. Neural Computation, 13(7), 1443-1471.

[24] Song, Q., Hu, W., & Xie, W. (2002). Robust support vector machine with bullet hole image classification. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 32(4), 440-448.

[25] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. In 2008 Eighth IEEE International Conference on Data Mining (pp. 413-422). IEEE.

[26] Ramirez-Asis, E., Bolivar, R. P., Gonzales, L. A., Chaudhury, S., Kashyap, R., Alsanie, W. F., & Viju, G. K. (2022). A lightweight hybrid dilated ghost model-based approach for the prognosis of breast cancer. Computational Intelligence and Neuroscience, 2022, 1–10.

[27] Mohanakurup, V., Parambil Gangadharan, S. M., Goel, P., Verma, D., Alshehri, S., Kashyap, R., & Malakhil, B. (2022). Breast cancer detection on histopathological images using a composite dilated Backbone Network. Computational Intelligence and Neuroscience, 2022, 1–10.

[28] Nair, R., Alhudhaif, A., Koundal, D., Doewes, R. I., & Sharma, P. (2021). Deep learning-based COVID-19 detection system using pulmonary CT scans. Turkish Journal of Electrical Engineering & Computer Sciences, 29(SI-1), 2716–2727.

[29] Shah, S. A. A., Uddin, I., Aziz, F., Ahmad, S., Al-Khasawneh, M. A., & Sharaf, M. (2020). An Enhanced Deep Neural Network for Predicting Workplace Absenteeism. Complexity, 2020, Article ID 5843932, 1-12. doi: 10.1155/2020/5843932.

[30] Uddin, M. I., Shah, S. A. A., & Al-Khasawneh, M. A. (2020). A Novel Deep Convolutional Neural Network Model to Monitor People following Guidelines to Avoid COVID-19. Journal of Sensors, 2020, Article ID 8856801, 1-15. doi: 10.1155/2020/8856801.

[31] Kashyap, R. (2022a). Big Data and Global Software Engineering. In Research Anthology on Big Data Analytics, Architectures, and Applications (pp. 1249–1274). Retrieved from https://doi.org/10.4018/978-1-6684-3662-2.ch060.

Doi : https://doi.org/10.54216/JCIM.120203
Received: December 18, 2022 Revised: February 18, 2023 Accepted: May 19, 2023