ENHANCING CYBER-SECURITY FOR 5G NETWORK: A FOCUS ON THREAT DETECTION TECHNIQUES

[1]Nweke Okwuchukwu A., [2]Ugwu Edith A., [3]Asogwa Tochukwu C.,[4]Kwubeghari A.
[1,2,3,] Department of Computer Science; [4]Department of Computer Engineering;
[1,2,3,4]Enugu State University of Science and Technology, Enugu State, Nigeria
[1]austinokey83@gmail.com;[2]edith.ugwu@esut.edu.ng, [3]tochukwu.asogwa@esut.edu.ng;
[4]kwubeghari@gmail.com

Article Info
Received: 11/9/ 2023
Revised: 7/11/2023
Accepted 28/11/2023

Corresponding Author's
Email::austinokey83@gmail.con

Corresponding Author's
Tel:+2348101721921

ABSTRACT

This study explores the evolution of wireless technology from 1G to 5G, highlighting the progress and benefits of 5G networks, including faster data speeds, low latency, and support for a massive number of connected devices. Review of literatures on 5G network based threat detection techniques, including machine learning, encryption, and other methods. It specifically discusses the use of artificial neural networks for black-hole attack detection and presents results, including accuracy, precision, sensitivity, and specificity, after the neural network model was trained with optimization technique. Comparative analysis with other models reveals the effectiveness of neural networks in cyber threat detection. Overall, the study contributes to the knowledge of 5G technology and its security challenges while highlighting the potential of machine learning techniques for threat detection in 5G networks.

Keywords: 5G, Security challenges, Cyber-Attacks, Neural Network, Threat Detection

1. INTRODUCTION

The evolution of wireless technology from 1G to 5G has been a remarkable journey. It all began with the first Generation (1G), the 1G of mobile networks introduced in the 1989s, which enabled basic voice calls. Then came Second Generation (2G) in the 1990s, According, to (Sanjay and Neeraj, 2018), they revealed that the 2G was based on digital technology and provides much better spectrum efficiency and security. The early2000s witnessed the advent of the Third Generation (3G), which introduced mobile internet access and multimedia capabilities. This was followed by the Fourth Generation(4G) in the late 2000s, offering faster speed and enabling the rise of mobile apps and video streaming. And now, we have the Fifth Generation, the latest generationwhich promises ultra-fast speeds, low latency, and massive connectivity to support advanced technologieslike autonomous vehicles, virtual reality, and smart cities. Each generation has built upon the previous ones, pushing the boundaries of what is possible in wireless communication. The benefits of 5G networks are numerous. According to (Emma and Peng, 2020), They revealed that the development of digital and telecommunication technologies increases the demand for multimedia content, such demand has been rapidly expanding over the years in the form of broadcasting, movies, internet, and personal media.5G offers significantly faster speeds, allowing for quick downloads, seamless streaming, and smooth browsing experiences. Furthermore, 5G provides lower latency, reducing delays and enabling real-time interactions, which is crucial for applications like autonomous vehicles and remote surgeries. Also, 5G supports a massive number of connected devices, making it ideal for the Internet of

Things (IoT) and smart cities, where countless devices need to communicate simultaneously. In addition, 5G networks offer improved reliability and network efficiency, ensuring a more stable and consistent connection. Finally, 5G has the potential to revolutionize various industries, such as healthcare, manufacturing, and entertainment, by enabling innovations like remote patient monitoring, smart factories, and immersive virtual reality experiences.Despite the success of the 5G network and its potential benefits pre-defined, the network also suffers certain quality of service constraints which include interference, congestion, and high cost of deployment, among others. Among this constraint, the issues of insecurity have continued to gain increased research attention over the years.Mishra (2021) reported several incidents of cyber-attacks on 5G networks, Mishra (2021) identified some of these attacks such as man in the middle attack, wormhole attacks, denial of service attacks, black hole attacks, etc. According to Bendovschi (2015), the reason for this attack includes Network slicing vulnerabilities, supply chain security, and lack of standardized protocols. Additionally, the cost of deploying and maintaining 5G networks can also be a significant challenge, along ensuring robust security of 5G networks is of utmost importance for their successful deployment and operation. with the enhanced connectivity and data transmission capabilities of 5G, it is crucial to have robust security measures in place to protect against cyber threats and ensure user data privacy. Therefore, this study seeks to investigate the challenges of existing 5G security models and make recommendations to address problems.

2. METHODOLOGY

The research methodology was centered on elucidating various network security techniques, encompassing Machine Learning, Encryption, and other methods. Within the realm of Machine Learning, the focus extended to encompass data collection, feature extraction, neural network architecture, propagation algorithms, traditional privacy protection mechanisms, intrusion detection systems, and advanced technologies such as Deep Learning (DL), Machine Learning (ML), Long and Short-Term Memory (LSTM), and Auto-Encoder (AE) architecture.In the domain of Encryption, the investigation delved into Evolved Packet System Authentication and Key Agreement (EPS-AKA), Extensible Authentication Protocol (EAP-AKA), Advanced Encryption Standard (AES) Algorithm, various cryptographic approaches, Physical Layer Security (PLS), RSA Encryption (RSA Enc), Data Encryption Standard (DES), Triple DES, and Secure Hash Algorithm 256 (SHA256).Additionally, the study explored a spectrum of other techniques, including Software Defined Networks (SDN), Network Function Virtualization (NFV), User Equipment (UE), Additive Manufacturing File Format (AMF) models, Device-to-Device communication, heterogeneous networks, massive multiple-input-multiple-output systems, software-defined networks, and the Internet of Things (IoT). Furthermore, it delved into Software Defined Networks, Modified Security Protocols IPsec, and various Cryptography protocols to provide a comprehensive overview of contemporary network security methodologies.Figure 1 presents a mind-mapping diagram of the various types of security models.

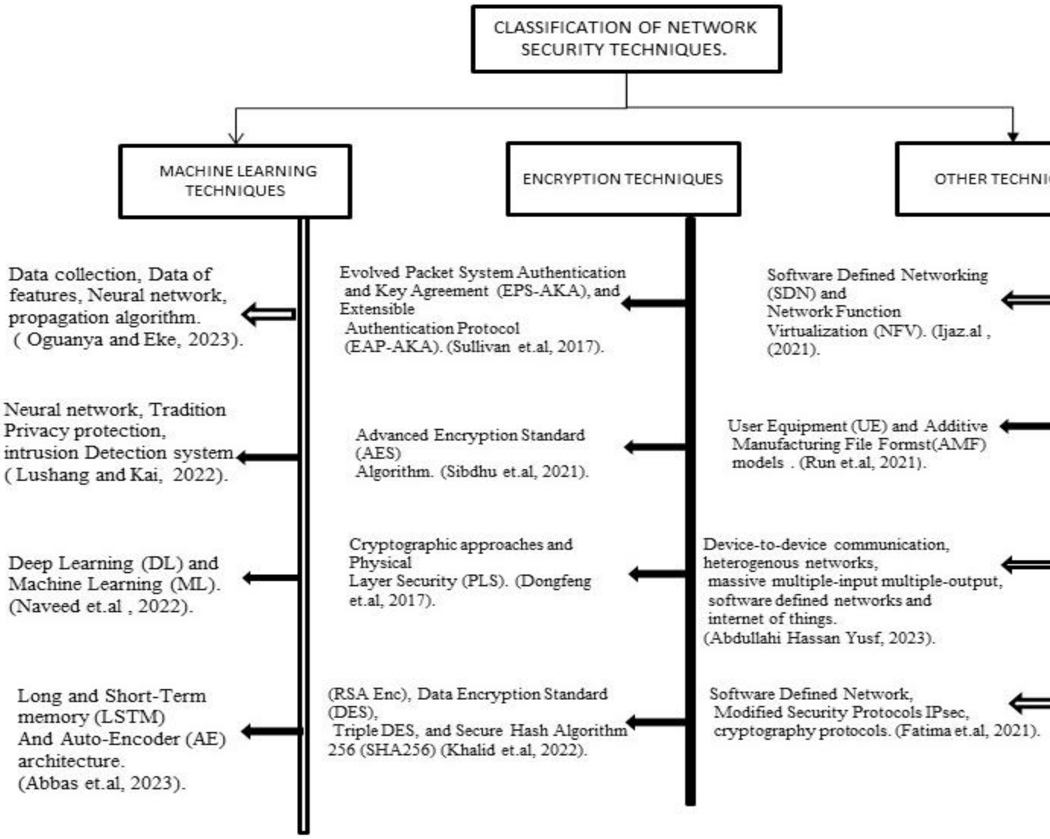

CLASSIFICATION OF NETWORK SECURITY TECHNIQUES.
MACHINE LEARNING TECHNIQUES
ENCRYPTION TECHNIQUES
OTHER TECHNIQUES
Data collection, Data of features, Neural network, propagation algorithm. (Oguanya and Eke, 2023).
Neural network, Tradition Privacy protection, intrusion Detection system (Lushang and Kai, 2022).
Deep Learning (DL) and Machine Learning (ML). (Naveed et.al , 2022).
Long and Short-Term memory (LSTM) And Auto-Encoder (AE) architecture. (Abbas et.al, 2023).
Evolved Packet System Authentication and Key Agreement (EPS-AKA), and Extensible Authentication Protocol (EAP-AKA). (Sullivan et.al, 2017).
Advanced Encryption Standard (AES) Algorithm. (Sibdhu et.al, 2021).
Cryptographic approaches and Physical Layer Security (PLS). (Dongfeng et.al, 2017).
(RSA Enc), Data Encryption Standard (DES), Triple DES, and Secure Hash Algorithm 256 (SHA256) (Khalid et.al, 2022).
Software Defined Networking (SDN) and Network Function Virtualization (NFV). (Ijaz.al , (2021).
User Equipment (UE) and Additive Manufacturing File Formst(AMF) models . (Run et.al, 2021).
Device-to-device communication, heterogenous networks, massive multiple-input multiple-output, software defined networks and internet of things. (Abdullahi Hassan Yusf, 2023).
Software Defined Network, Modified Security Protocols IPsec, cryptography protocols. (Fatima et.al, 2021).

Figure 1: The Classification of Network Security Techniques

2.1 MACHINE LEARNINGTECHNIQUES FOR CYBER SECURITY IN 5G

Oguanya and Eke (2023) addressed the problem of a black hole in wireless networks using artificial intelligence techniques in the study, the methods used are data collection, data of features, and artificial neural network for the development of black hole detection mode (Abdelhamid et. Al, 2023),thepropagationalgorithm was used for the neural network training and the result reported for regression is 0.99887 and mean square error of 0.00023665Mu when deployed on the wires network, the throughput reported 8.945%.Lushang and Kai (2022) deeply highlighted the wireless sensor network system based on neural networks, traditional privacy protection, and intrusion detection systems. they applied the particle swarm optimization algorithm to construct a wireless sensor network intrusion detection system.The systemconsistsof important modules such as data extraction, data analysis, data feedback, and auxiliary decision-making. In addition, the paper further enhances the wireless sensor network privacy protection scheme based on polynomial regression and a user privacy protection scheme based on the same state encryption.These schemes improve the security of privacy protection and facilitate information management.Naveed et.al (2022) stated that Network Intrusion Detection Systems (NIDS) prevent intrusions into a network and preserve the network's integrity, availability, and confidentiality (Desai et.al, 2023). In addition, some advanced approaches such as Deep Learning (DL) and Machine Learning were implemented in SDN-based NIDS to overcome the security issues within a network.Abbas et.al (2023) proposed an ensemble deep learning model that utilizes Long Short-Term Memory (LSTM) (Arifin et.al, 2023) and Auto-Encoder (AE) architecture (Chen and Guo, 2023) to identify out-of-norms activities for cyber threat hunting in Industrial Internet of Things (IIOT) (Kargakos, 2023). The LSTM is applied to create a model on normal time series of data (past and present data)to learn normal data patternsand important features of the data are identified by AE to reduce data dimension.The model was evaluated considering abnormal cyber threats and it reported a successful threat detection accuracy of 0.997.

2.2 ENCRYPTION TECHNIQUES THREAT DETECTION IN 5G

Sullivan, et al (2017) categorized security technologies using Open System Interconnection (OSI) and Layers. In the study, various layers of wireless network technologies were considered which are the application layer, physical layer, presentation layer, network layer, and data link layer. In addition, known vulnerabilities and attacks at these layers such as disclosure of user identity, Denial of service (DOS), and man-in-the-middle attacks were identified using Evolved Packet System Authentication and Key Agreement (EPS-AKA) (Abdradou et.al 2015), Extensible Authentication Protocol (EAP-AKA) (Edris et.al, 2022). Furthermore, security mechanisms such as noise interference, beamforming, and degrading signal reception were introduced to protect data from threats such as eavesdropping and data fabrication. Sibdhu et.al (2021) proposed a model that is suited for wireless network systems and devices. This model aims to identify, detect, categorize, and respond to attacks generating warnings and alarms in case any malicious activity is observed. known as the system model, it comprises a detection phase, response system, and system mechanism. The detection phase scans and classifies attacks based on risk level, distinguishing between known or anomalous attacks. Once an attack is detected, the system generates alerts, and warning messages and also identifies the source of the attack. The Incident response system is integrated with the detection system, allowing immediate recovery once an attack is identified. To ensure a strong security mechanism within network traffic, the security implements the Advanced Encryption Standard (AES) algorithm for data encryption (Mahanta, 2023), mitigating the risk of insider attacks or malicious activities causing data loss. Dongfeng et.al (2017) revealed an advanced feature of 5G wireless network systems, new security requirements, and challenges. the techniques used are heterogeneousnetworks, device-to-device communications, massive multiple-input multiple-output, software-definednetworks, and the Internet of Things. In addition, the study identified and categorized different types of attacks which are passive attacks and active attacks; Passive attacks violate data confidentiality and user privacy. while active attacks, on the other hand, involve the modification of data or interruption of legitimate communication. Furthermore, the research recommended cryptographic approaches and Physical Layer Security (PLS) (Shi et. al., 2022) approaches as the mechanism used to tackle security attacks.Khalid et.al (2022) examined an encryption algorithm that could be proposed to enhance data security in both 4G and 5G networks. These encryption algorithms offer a suitable level of data security in various applications. For example, certain encryption algorithms like (RSA Enc), Data Encryption Standard (DES), Triple DES, and Secure Hash Algorithm256 (SHA256) have been utilized for data security in Software-DefinedNetworks (SDN) (Aziz and Abdulqadder, 2021). Additionally, encryption algorithms such as Advanced Encryption Standard (AES) (Mahanta, 2023), Revest Cipher6 (RC6) (Auxillia 2016), Twofish, Simon and Speck lightweight Block Ciphers (SPECK), and chacha20 were employed for data security in Internet of Things (IoT devices) (Jasim et.al, 2021). Moreover, the Basic components of the encryption algorithm include the (Universal Cryptography Algorithm (ZUC) cipher algorithm, SNOW 3G cipher algorithm, and AES cipher algorithm). Furthermore, the ZUC algorithm requires two keys; a 128-bit secret encryption key (K) and a 128-bit initialization vector key (IV key). The SNOW 3G algorithm relies on a secret key (K= 128 bits) and an IV key (IV= 128 bits), while the AES algorithm depends on a secret encryption key (K,K =128 bits) and a counter block (T,T = 128 bits).

2.3 OTHER TECHNIQUES FOR THREAT DETECTION IN 5G

Ijaz et. (2017) highlighted the basic challenges in 5G, such as Denial of services (DOS) attacks on end-user devices, signal storm, DOS attacks on infrastructure, roaming security, mandated in the network, security of radio interfaces and flash network traffic, Additionally, the mechanisms used to eliminate these challengesincludes Software Defined Networking (SDN) (Nunez et.al, 2023) and Network Function Virtualization (NFV). SDN was used to enable the run-time resources, such as bandwidth, and assignment to specific network parts as needed. Using the NFV, services from the core network cloud can be transferred to the edge to meet user requirements.Run et.al (2021) applied the User Equipment (UE) (Adikpe et.al, 2022) and Additive Manufacturing File Format (AMF) models into two synchronous communication finite state machines to improve the quality of services in 5G. The study extracted the desired properties from relevant 3GPP specifications. The research demonstrated that the null security algorithm used in normal communication poses a security threat in the 5G network. This algorithm can potentially lead to IP spoofing attacks and Unique Subscription Permanent Identifier (SUPI) catching attacks. Additionally, the researchers analyzed the root cause of these network attacks such as the encryption and integrity of the wireless air interface are not strong enough, furthermore, an anomaly detection method called adversary consumption was proposed to prevent such attacks from being launched.Abdullahi (2023) highlighted fundamental challenges in this study, including Denial of Service (DOS) attacks on the end-user devices, flash network traffic, roaming security, user plane integrity, Denial of Service (DOS) attacks on the infrastructure, signaling storms, and security of radio interfaces. Additionally, the study delves into the new security features that involve different technologies applied in 5G, such as device-to-device communication (Sarka and Gupta, 2020), heterogenous networks (Zhao et.al, 2023), massive multiple-input multiple-output, software-defined networks (Nunez et.al, 2023), and the Internet of things.Fatima et.al (2021) listed the challenges of 5G. They mentioned that spoofing attacks are a concern, as 5G is vulnerable to such attacks due to its operation with high-power servers and underutilized resources. Additionally, they highlighted that traffic steering-based machine learning in V2X allows efficient peak management over the data center, but it may result in a single target being overwhelmed, leading to Denial Of Service (DOS) and resource drain. Furthermore, the study proposed some techniques to secure the 5G network. One of these techniques is SDN (Nunez et.al, 2023), which can identify attacks over the network flows, states, and resources through traffic analysis and response systems. Another technique mentioned is the use of modified security protocols IPsec and cryptography protocols to secure communication channels in 5G.

3. ARTIFICIAL NEURAL NETWORK

In this study, Figure 1 illustrates the classification of network security and techniques. various approaches including machine learning, encryption, and other techniques, were considered. Based on the survey, machine learning was identified as the best option due to its accuracy and performance. To this end, the neural network was adopted asthe preferred machine learning method for developing the cyber threat detection system. A neural network is a computational model inspired by the structure and functioning of the human brain. Itconsists of interconnected nodes called neurons, organized layers. Each neuron has associated weights and biases. Weight determines the strength of connections between neurons, while biases adjust the output of each neuron. Therectified linear unit activation function determines whether a neuron should be activated or not based on the weighted sum of inputs and biases. It introduces non-linearity to the network, allowing it to earn complex patterns and make predictions.

3.1 ModelingNeural Network Threat Detection System

To develop the threat detection model, data of black-hole was collected from Afrihub center, Enugu Nigeria containing 5 major attributes as presented in Table 1;

Table 1: Data Attributes

S/N	Attributes	Data type
1	Target IP address or range	String
2	Traffic redirection technique	Packet-level data
3	Type of traffic affected	Qualitative data
4	Duration of the attack	Qualitative data
5	Goals of the attack	Qualitative data

The data collected was imported into the neural network and trained using an optimization algorithm to formulate a model that can generalize and make accurate predictions on new, unseen data.

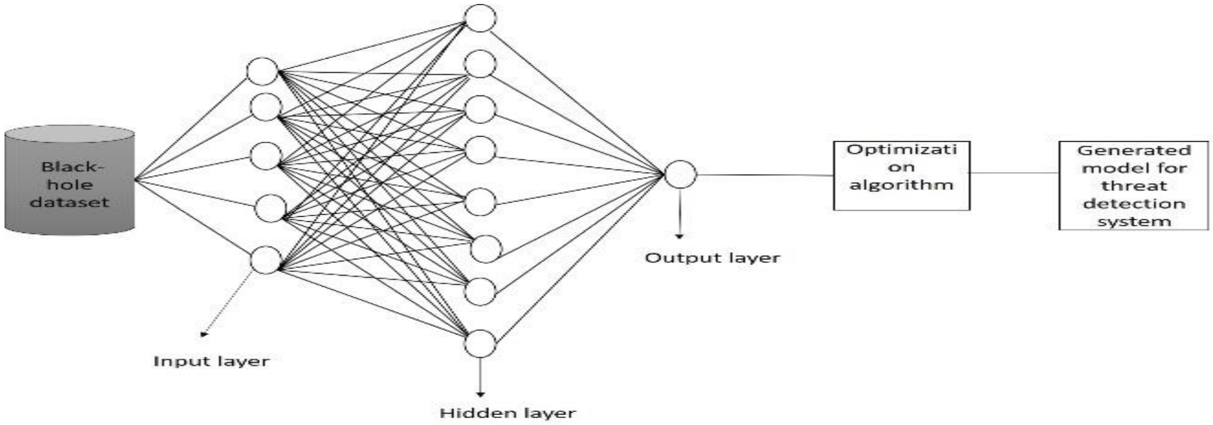


Figure 2: Neural network architecture

Figure 2 presents a visual narrative of the neural network training. The data collected was channeled into the neural network and then trained using an optimization algorithm to generate the model for an advanced threat detection system. The model portrays the intricate interplay between the input data and the neural network's architecture, emphasizing the sequential steps involved in transforming the raw information into a discerning threat detection framework. The optimization algorithm refines the network parameters, fine-tuning its synaptic connections and weights to bolster its capacity in accurately discerning potential threats within the data.

3.2 Results and Discussions

This section presented the result of the neural network for the classification of threat detection systems. The Receiver Operating Characteristic (ROC) curve serves as a crucial tool in assessing the effectiveness of an Artificial Neural Network (ANN) model designed for Intrusion Detection Systems (IDS) within the intricate landscape of a 5G network. This graphical representation illustrates the model's performance across various thresholds by plotting the true positive rate against the false positive rate in the ROC of Figure 3.

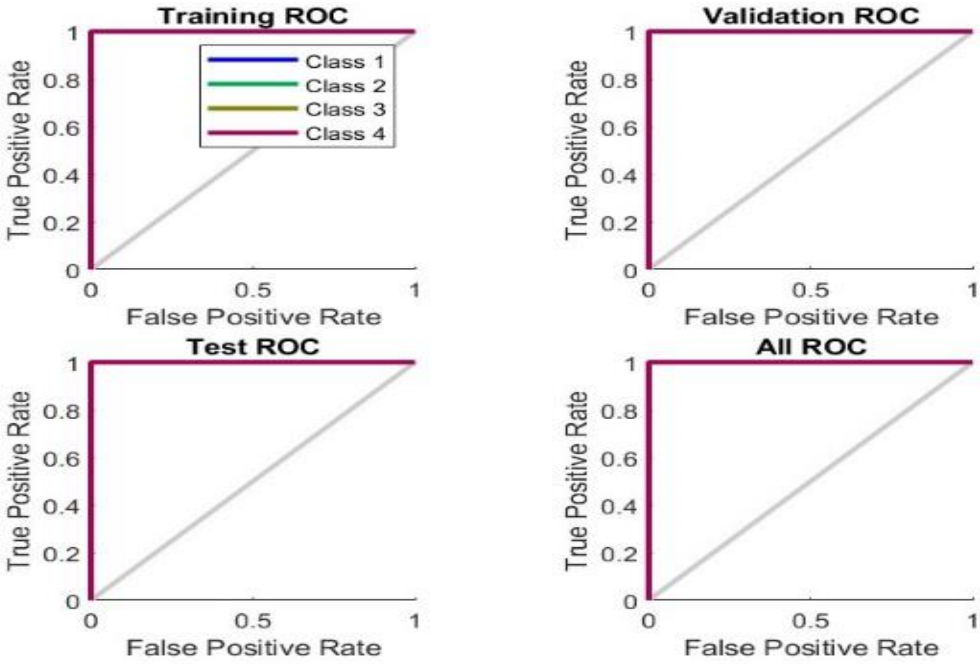


Figure 3: The ROCcurve

The ROC curve aims to achieve a value that is close to 1, ROCrepresents the relationship between the true positive rate and the false positive rate. The true positive rate refers to correct classifications, where an attack is tested and correctly detected. The false positive rate refers to incorrect classifications, where an attack is not detected. Similarly the cross entropy performance was also graphically analyzed and the results presented in the figure 4;

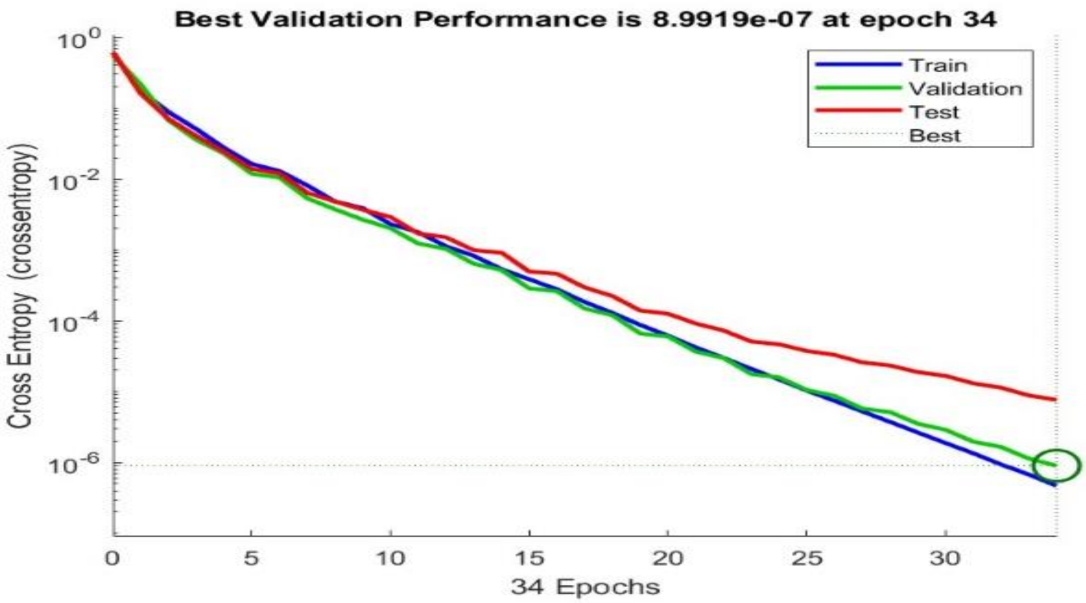
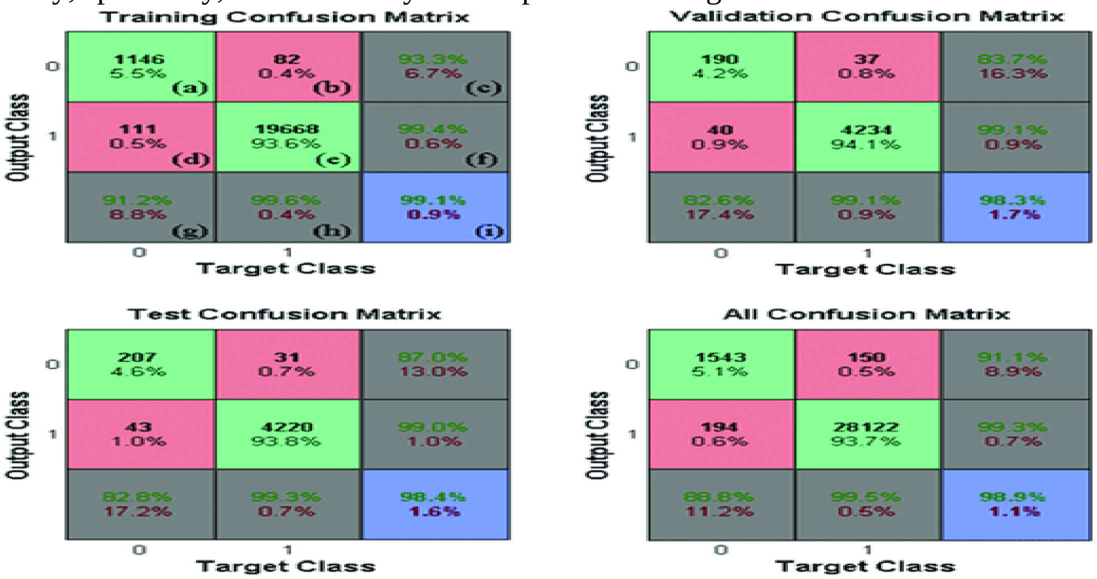


Figure 4: Thecross-entropy

The cross-entropy of the threat detection system model, the error reported after validation is 8.9919e-07 and at epoch 34. This indicates that, on average, the neural network's predictions are relatively close to the true labels for the given set of threat detection systems at that particular epoch. In addition, it implies that the neural network has learned to make more accurate predictions of threat detection.The next result utilized a confusion matrix to evaluate the threat detection system model's prediction. The confusion matrix is a table that provides a detailed breakdown of the threat detection system. It helps to assess various metrics such as precision, accuracy, specificity, and sensitivity were reported as in Figure 5:



Training Confusion Matrix

Output Class	0	1	
0	1146 5.5% (a)	82 0.4% (b)	93.3% 6.7% (c)
1	111 0.5% (d)	19668 93.6% (e)	99.4% 0.6% (f)
	91.2% 8.8% (g)	99.6% 0.4% (h)	99.1% 0.9% (i)

Target Class

Validation Confusion Matrix

Output Class	0	1	
0	190 4.2%	37 0.8%	83.7% 16.3%
1	40 0.9%	4234 94.1%	99.1% 0.9%
	82.6% 17.4%	99.1% 0.9%	98.3% 1.7%

Target Class

Test Confusion Matrix

Output Class	0	1	
0	207 4.6%	31 0.7%	87.0% 13.0%
1	43 1.0%	4220 93.8%	99.0% 1.0%
	82.8% 17.2%	99.3% 0.7%	98.4% 1.6%

Target Class

All Confusion Matrix

Output Class	0	1	
0	1543 5.1%	150 0.5%	91.1% 8.9%
1	194 0.6%	28122 93.7%	99.3% 0.7%
	88.8% 11.2%	99.5% 0.5%	98.9% 1.1%

Target Class

Figure 5:The confusion matrix

The confusion matrix in figure 5 reveals that the accuracy reported is 98.9%, this means that the generated threat-detectingmodel can correctly detect black-hole attacks with 98.9% accuracy. In addition, the precision reported is88.8%, indicating that out of all the cases identified as threats by the classification model, 88.8% of the threats were true. Similarly, sensitivity was reported at 91.1%, in this case, the threat-detectingmodel successfully identified 91.1% of the true threats present. Furthermore, the specificity reported is 99.3%, indicating that the threat-detecting model accurately identified 99.3% of non-threat presents.

Table 1: Validation of threat-detecting system

S/N	ACCURACY(%)	PRECISION(%)	SENSITIVITY(%)	SPECIFICITY (%)
1	98.9	88.8	91.1	99.3
2	98.8	91.1	88.5	95.9
3	98.9	91.9	94.5	97.2
4	99.5	93.2	93.1	99.9
5	97.9	90.9	91.2	97.6
6	99.6	89.3	90.4	98.3
7	98.7	89.9	92.1	99.2
8	99.4	92.8	97.6	98.3
9	98.8	92.2	89.1	98.7
10	99.7	90.8	90.1	96.9
Avg.	99.02	91.09	91.77	98.13

Table 1 provides a comprehensive overview of the validation metrics for the threat-detecting system, offering an insight into its performance across various key parameters. The accuracy metric, denoting the overall correctness of the system, consistently exhibits a high average of 99.02%, underscoring the system's reliability in making correct predictions. Precision, representing the system's ability to avoid false positives, maintains a commendable average of 91.09%, indicating a strong capability in accurately identifying actual threats without undue alarms.Sensitivity, crucial for capturing true positives, boasts an average of 91.77%, reflecting the system's adeptness in identifying genuine threats within the dataset. Specificity, measuring the system's proficiency in avoiding false negatives, exhibits a robust average of 98.13%, highlighting the system's effectiveness in discerning non-threat instances accurately. The individual performance across the ten scenarios is notably consistent, with each showcasing a balance between precision and sensitivity. This collective evaluation, culminating in the averages, attests to the threat-detecting system's high overall performance and reliability, positioning it as a potent tool in fortifying the security apparatus of the 5G network it safeguards.

4. CONCLUSION

The evolution of wireless technology from 1G to 5G has brought remarkable advancements in communication, offering faster data speeds, lower latency, and support for various applications. However, the benefits of 5G are accompanied by security challenges, including cyber threats like man-in-the-middle attacks and denial-of-service attacks. To address these issues this research explored techniques such as machine learning, encryption, and other method. This study emphasizes the effectiveness of machine learning, particularly artificial neural networks, in detecting and mitigating these threats with exceptional accuracy and precision. As 5G technology continues to evolve, robust security measures and innovative threat detection systems are crucial to ensure the network's integrity and safeguard against emerging cyber threats, contributing significantly contribution to the field of 5G cybersecurity.

5. REFERENCE

AakifKuhafa, Gihan Niroshan and NadeeshaRajakarunarante (2022) "Cryptography in 5G- mini research paper," pp: 2, https://www.researchgate.net.

Abbas Yazdinejad, Mostafa Kazemi, Reza M. Parizi, Ali Dehghantanha and Hadis Karimipour (2023) " An ensemble deep learning model for cyber threat hunting in the industrial internet of things" Digital Communications and Network volume 9, pp:1-9, https://doi.org/10.1016/j.dcan.2022.09.008

AgburuOgahAdikpe, Patrick Udeh Okorie, Fraklin C Njoku, Matthew Iyobhebh (2022), "A hybrid user equipment mobility tracking scheme for minimizing the power consumption in location management procedures in 5G. https://www.icaens.org/

Alexander Nunez, Joseph Ayoka, Md ZahidulIsalm and Pablo Ruiz (2023), "A brief overview of software-defined networking.

AndreeaBendovshi (2015). "Cyber-Attacks – Trends, Pattern, and Security Countermeasures, 7th International Conference on Financial Criminology, https://www.sciencedirect.com.

Ashraf Abdelhamd, Mahmoud Said Elsayed, Anca D Jurcut, and Marianne A. Azer (2023). "A lightweight anomaly detection system for black hole attack" https://www.researchgate.net.

Auxilla A. (2016), "Rivest Cipher 6 (RC6)" school of information and technology engineering, VIT University, Vellore (DT)-632014, Tamil Nadu April 21, 2016. https://.www.researchgate.net.

Awad, W; ELseuofi, S. Machine learning methods for spam e-mail classification. Int. J. Comput. Sci. inf. Technol. 2011, 3, 173-184.

Demetra Kargalos (2023), "Industrial internet of thing (IIOT) AEC- (LEAD2)" https://www.champlainsaintlambert.ca

Dongfeng Fang, Yi Qian, and Rose Qingyang Hu (2017). "Security for 5G Mobile Wireless Networks" Faculty Publication from the Department of Electrical and Computer Engineering. https://www.digitalcommons.uni.edu.

Ed K. Kiyemba Edris, Mahdi Aiash and Jonathan Kok-keong Loo (2022), "Formalization and evaluation of EAP-AKA protocol for 5G network access security, https://doi.org/10.1016/j.array.2022.100254.

Fatima Salahdine,Tao Han, Ning Zhang (2022) "Security in 5G and beyond recent advances and future challenges,Security Challenges bin 5 G network" Dept of MSCSE, United International University.

Feng, P.; Ma, J.; Sun, C.; Xu, X.; Ma, Y.J.I.A. A Novel Dynamic Android Malware Detection System with Ensemble Learning. IEEE Access 2018, 6, 30996–31011.

I. Aziz and I. Abdulqadder (2021), "An overview on SDN and NFV security orchestration in a cloud network environment.

Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtovk (2017). "5G Security: Analysis of Threats and Solutions", DOI: 10.1109/CSCN.2017.8088621, 2017 IEEE conference on standards for communication and networking (CSCN), https://www.researchgate.net.

Jain, G.; Sharma, M.; Agarwai, B. Spam detection on social media using semantic convolutional neural network. Int. J. Knowl. Discov. Bioinform. 2018, 8, 12-26.

Jamil, Q.; Shah, M.A. Analysis of machine learning solutions to detect malware in Android. In proceedings of the 2016 Sixth International Conference on Innovation Computing Technology (INTECH), Dublin, Ireland, 24-26 August 2016; pp. 226-232.

K. Jassim, R. Ismail, A. Nahi AI-Rabeeah, and S. Solaimanzadeh (2021). "Analysis of the structure of some symmetric cipher algorithm suitable for the security of IoT Devices" Cihan University-Erbil Scientific Journal 5(2):13-19, DOI: 10.24086, pp13-19, https://www.research.net.

Karthika, R.; Visalakshi, P.J.W.T.C. A hybrid ACO-based feature selection method for email spam classification. WSEAS Trans. Comput. 2015, 14, 171-177.

Khalid Jassim, KayhanZrar Ghafoor, HalgurdSarhangMaghdid (2022). "Analysis of Encryption Algorithms proposed for data security in 4G and 5G generation", https://doi.org/10.1051/itmconf/20224201004.

Kwon, D.; Kim, H.; Kim, J.; Suh, S.C; Kim, I.; Kim, K.J. A survey of deep learning-based network anomaly detection. Clust. Comput. 2019, 22, 949-961.

Lusheng Shi and Kai Li (2022), "Privacy Protection and Intrusion Detection System of Wireless Sensor Network Based on Artificial Neural Network" https://doi.org/10.1155/2022/1795454.

Mahanta K. (2023), " An enhanced advanced encryption standard algorithm" International Journal of Advanced Trends in Computer Science and Engineering (IJATSCE), Vol 4, PP: 1-4, ISSN:2278-3091.

Malik, A.J.; Khan, F.A. A hybrid technique using binary particle swarm optimization and decision tree using behavior analysis for preventing APT attacks. J. Supercomput. 2017, 73, 2881-2895.

Mishra, S. K., Chowdhary, R., Kumari, S. and Rao, S. B. (2017). Effect of cell phone radiations on orofacial structures: a systematic review. J. Clin. Diagn. Res, 11(5): 5 - 12.

Mohammed ABDRABOU, Dr. Essam Abd El-wanis and Ashraf Elbayoumy (2023), “Security Enhancement for LTE Authentication Protocol (EPS-AKA), international conference on Aerospace Sciences and Aviation Technology, 16(AEROSPACE SCIENCES): 1-10, DOI:10.21608/asat.2015.23028, https://.www.researchgate.net.

Najadat, H.; Abdulla, N.; Abooraig, R.; Nawasrah, S. Mobile SMS am filtering based on missing classifiers. Int. J. Adv. Comput. Res. 2014, 1, 1-7.

Naveed Ahmed, Johan Mohamad Shatif, Saddam Hussain, Muhammad Siraj Rathore, Mueen Uddin, Asri bin Ngadi, Jawaid Iqbal, MahaAbdelhaq, RaedAlsaqour, Syed Sajid Ullah and Fatima TulZuhral (2022). “Network Threat Detection Using Machine/Deep learning in SDN-Based Platforms: A Comprehensive Analysis of state-of-the-Art Solution, Discussion, Challenges, and Future Research Direction”.

Naz, S.; Singh, D.K. Review of Machine Learning Methods for Windows Malware Detection. In proceeding of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICT), Kanpur, India, 6-8 July 2019; pp.1-6.

Ogbuanya I.M and Eke James (2023), Detection and isolation of black-hole in the wireless broadband ecosystem using artificial intelligence.

Pervez, M.S.; Farid, D.M. Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In proceeding of the 8th international conference on Software, Knowledge, Information, Management, and Applications (SKIMA 2014), Dhaka, Bangladesh, 18-20 December 2014l; pp 1-6.

Pranjail Desai, Avantika Sonawane, Tanvi Mane and Rupesh Chandrakant Jaiswal (2023), “Network-based intrusion detection system” https://www.researchgate.net.

Renuka, D.k.; Visalakshi, P.; Sankar, T.J.I.J.C.A. Improving E-mail spam classification using ant colony optimization algorithm. Int. J. Comput. Appl. 2015, 2, 22-26.

Run Zhang, WenAn Zhou, and Huamiao Hu (2021) “Towards 5G Security Analysis against Null Security Algorithms Used in Normal Communication” https://doi.org/10.1155/2021/4498324.

Samuel Arifin, AndryanKalmeRr, RindaNariswari and AnomYudistira (2023), “Long short-term memory (LSTM): Trends and future research potential” International Journal of Emerging Technology and Advanced Engineering, www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 certified Journal, volume 13.

Sanjay Sharma and Neeraj Sharma (2018), “An Overview of 5G Technology” International Journal of Engineering Research & Technology (IJERT).

Shuangshuang Chen and Wei Guo (2023), “Auto-Encoder in deep learning – A review with new perspectives” https://www.researchgate.net

Sindhu N Pujar, Gaurav Choudhary, Shishir Kumar Shandilya, Vikas Sihag, and Arjun Choudhary (2021) “An Adaptive Auto Incident Response based Security Framework for

Wireless Network Systems" Research Briefs on information and communication Technology Evolution 7:35-9, DOI: 10.5680/rebate.v7i.116.

Stein, G.; Chen, B.; Wu, A.S.; Hua, K.A. Decision tree classifier for network intrusion detection with GA-based feature selection. In Proceedings of the 43rd Annual Southeast Regional Conference-volume 2; ACM: New York, NY, USA, 2005; pp. 136-141.

Sufen Zhao, Rong Peng, Po Hu and Liansheng (2023), "Heterogenous Network embedding: A Survey" computer modeling in engineering and sciences 137 (1): 1-48, DOI:10:32604/cmes.2023.024781.

Sullivan, S. &Brighente, Alessandro & Kumar, Sathish & Conti, M. (2021). 5G Security Challenges and Solutions: A Review by OSI Layers. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3105396.

SumitSarka and Ridwan (2020), "Device to device communication" Sumit Sarkar, International Journal of Advanced Trends in Computer (IJATCA), special issues 1(2), April-2020, pp.18-21, ISSN: 2395-3519.

Vinayakumar, R; Alazab, M;Soman, K; Poornachandra, P; Al-Nermet, A.;. Venkatraman, S.J.I.A. Deep learning Approach for intelligent intrusion Detection System. IEEE Access 2019, 41525-41550.

Weiping Shi, Xinyi Jiang, Jinsong Hu, Abdeldime Mohamed Salih Abdelgader (2022), "Physical layer security techniques for data transmission for future wireless networks" Security and safety, Vol. 1, 2022007. pp: 1-30; https://doi.org/10.1051/sands/2022007.

Zhang, Y.; Li, P.; Wang, X.J.I.An Intrusion detection FPR IoT based on an improved genetic algorithm and deep belief network. IEEE Access 2019, 7, 31711-31722.