Amrita School of Engineering, Bengaluru
Department of ECE
B. Tech. AY 2023-2024 (VII Semester)
Objective Details – 19EAC401- Cyber Security

Group Number: 5

Name of the Students:

Name	Roll No
Ruthwik N M T	BL.EN.U4EAC20064
Suyash Mishra	BL.EN.U4EAC20077
T K Luchingba	BL.EN.U4EAC20080

Abstract:

Network security must extend its protective umbrella to embrace the virtualization layer, ensuring that virtualized components remain resilient to attacks. Virtualization security in turn, must align with network security practices to fortify the integrity of virtualized environments. Together, they create a fortified digital foundation upon which vRANs can thrive. Conversely, vRANs must adhere to the security principles set by both domains, safeguarding against threats while delivering the promise of high-performance wireless connectivity.

This abstract explores the interconnectedness of network security, virtualization security, and vRANs, emphasizing that in the modern telecommunications landscape, security is not a singular concern but a harmonious symphony that underscores the trust, reliability, and resilience of our digitally connected world.

Network Security: Network security remains the linchpin in an increasingly interconnected world. It serves as the guardian of data, applications, and the very fabric of modern communication. Threats, ranging from cyberattacks to data breaches, continuously evolve in sophistication. Network security strategies encompass threat detection, access control, encryption, and security policies. These measures, bolstered by advanced technologies like machine learning and behavioral analytics, form the first line of defense in safeguarding our connected world.

Virtualization Security: The advent of virtualization technologies has redefined how IT resources are managed and allocated. The ability to abstract and virtualize hardware resources has opened new frontiers in scalability and resource optimization. Yet, it brings forth novel security challenges. Securing virtual machines, containers, and hypervisors requires robust practices to ensure isolation, integrity, and availability. Virtualization security extends beyond traditional perimeters to encompass the very heart of digital infrastructure.

vRAN (Virtual Radio Access Networks): As 5G networks emerge as the backbone of our hyperconnected world, vRANs have taken center stage. Leveraging virtualization, vRANs orchestrate radio access functions with unprecedented flexibility and scalability. They optimize resource allocation, improve interference management, and redefine the economics of wireless networks. However, this architectural revolution ushers in a new frontier of security challenges. Protecting virtualized network functions, securing wireless transmissions, and preserving data privacy in a vRAN context demand innovative solution.

Amrita Vishwa Vidyapeetham
School of Engineering, Bengaluru
Department of Electronics and Communication Engineering
19EAC401 -Introduction to Cyber Security

Group	**:**	ENIGMA (TEAM 5)
Title of the Project	**:**	Intrusion detection in 5G networks using LSTM

Team Details
BL.EN.U4EAC20064 : Ruthwik N M T
BL.EN.U4EAC20077 : Suyash Mishra
BL.EN.U4EAC20080 : T K Luchingba

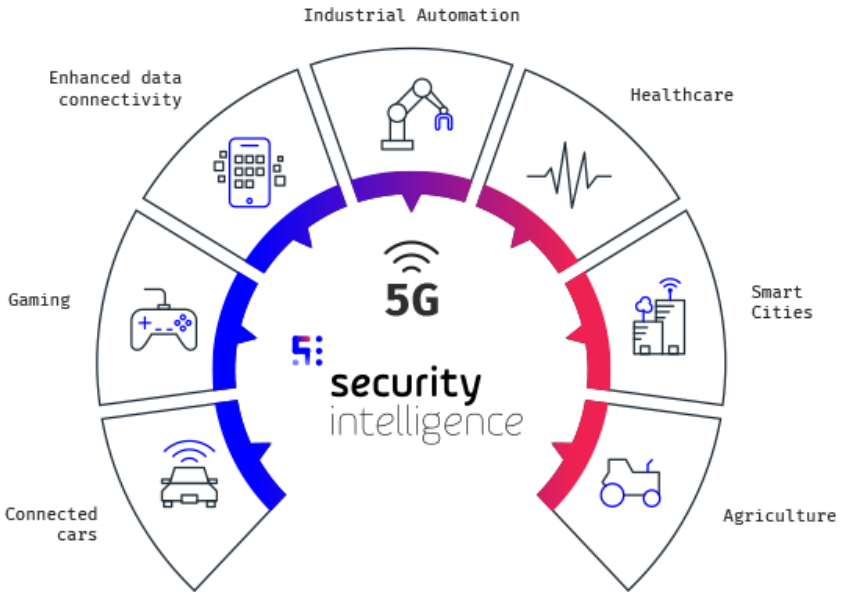
Tools: Python, HTML, CSS, Java Script

Write-up of the project:

In recent years, there have been notable advancements in cyber security defense systems, which have introduced innovative approaches and new Intrusion Detection Systems (IDS). These IDS are now capable of identifying cyber-threats that were previously undetectable. However, the imminent fifth-generation (5G) mobile technology comes with a fresh set of challenges for protection. The project proposes a 5G-centric architecture designed for the efficient and rapid analysis of network traffic, specifically tailored to identify cyber-threats within 5G mobile networks which is achieved by harnessing deep learning techniques.

This study explores the feasibility of using ML neural networks for identifying cyberattacks. It introduced the idea of employing mobile edge computing to enhance security by collecting network traffic data from the **Radio Access Network (RAN)** and detecting potential malicious activity on the mobile edge, enabling faster threat detection.

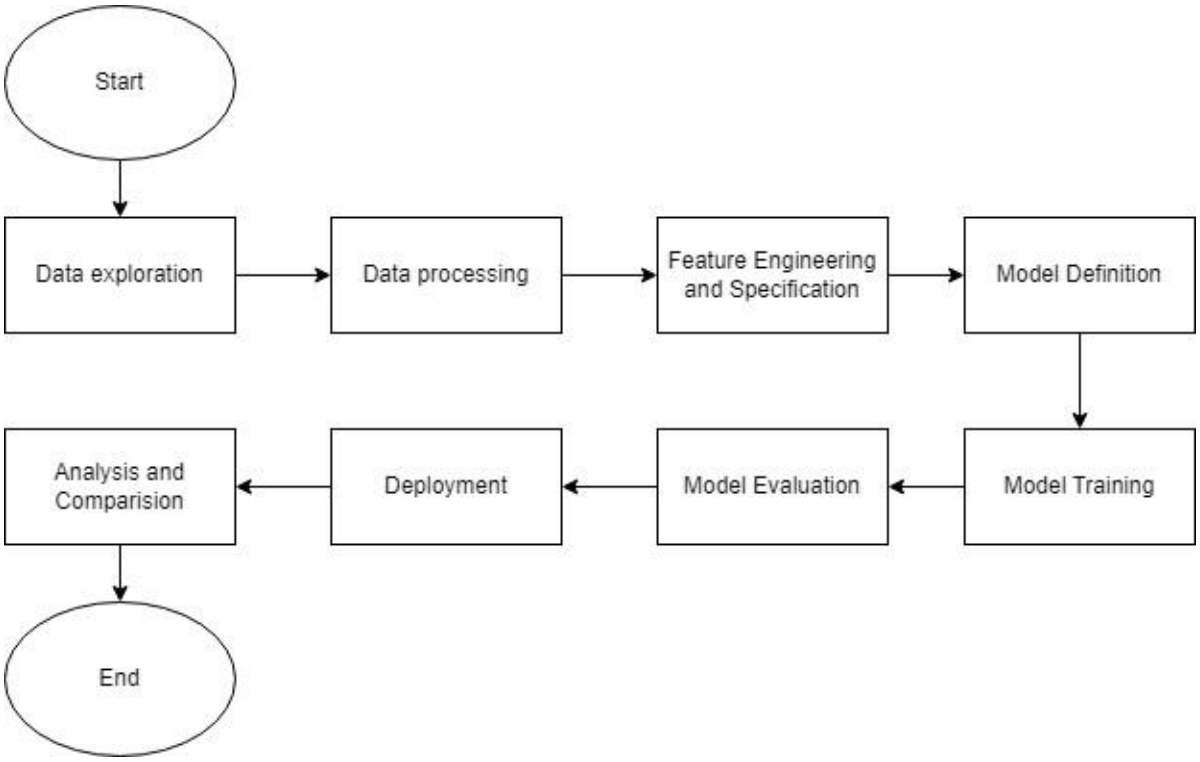
Additionally, this project aims to implement an "armed microservices" strategy. Under this approach, each microservice is equipped with its Machine Learning algorithm and training data. These microservices are deployed to defend against various threat categories, including DOS, U2R, R2L, probe attacks, as well as telecom-specific threats like M3UA threats, SMS fraud, and spam.



Dataset:
http://www.di.uniba.it/~andresini/datasets.html#:~:text=NSL%2DKDD%20is%20a%20new,compare%20different%20intrusion%20detection%20methods.

Technologies:

- **ASD**: Anomaly Symptom Detection, situated within the Radio Access Network (RAN) infrastructure, is dedicated to swiftly identifying any signs or traces of anomalies in the network traffic generated by User Equipment (UE) connected to the RAN, employing a fully connected Deep Neural Network.
- **NAD**: Network Anomaly Detection serves as a repository for timestamped symptoms associated with the RAN, collected and forwarded by the ASDs. Upon detecting an anomaly, it is promptly relayed to the Monitoring and Diagnoser module and employs an RNN LSTM network for its operations.
- Diagnose and Policy Server is **a graphical user interface (GUI)** environment designed to create visual representations of interconnected infected devices and, in cases of botnets, identify the controlling botmasters. It equips experts with the ability to delve deeper into the flow of data packets and take proactive measures to prevent potential security threats.



19EAC401- CYBER SECURITY	GROUP 5: ENIGMA	
SL.NO	PAPER NAME	INFERENCE
1	A Network Security Situation Element Extraction Method Based on Conditional Generative Adversarial Network and Transformer.	This paper underscores the importance of mitigating sample imbalance in network traffic data, utilizing CGAN(Conditional Generative Adversarial) to enhance accuracy. It introduces Transformer to further boost accuracy and highlights its underutilized potential in feature extraction. The proposed method outperforms existing approaches in terms of detection accuracy and is versatile across different datasets.
2	A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security	This study highlights the vital role of security in wireless sensor networks (WSNs) for data protection and system efficiency. It covers key security aspects like secure key exchange, user authentication challenges, and methods for detecting malicious intentions. Additionally, it stresses the importance of secure localization and self-organization in WSNs, emphasizing measures such as MAC protocols and digital signatures for data integrity. Overall, the paper offers a comprehensive approach to fortifying WSN security against potential threats.
3	Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats	This paper introduces a novel security operation center (SOC) and emphasizes requirements and integration with optical-layer control. It explores efficient ML techniques, combining unsupervised and semi-supervised learning with dimensionality reduction, analyzing accuracy versus runtime trade-offs. The paper suggests using blockchain for model privacy and trustworthiness, highlights attack localization precision, and underscores the value of unsupervised learning (e.g., DBSCAN) and dimensionality reduction (e.g., autoencoders) for anomaly detection and data visualization in optical network security management.
4	Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges	This paper explores security and privacy challenges in 6G wireless networks with a focus on reconfigurable intelligent surfaces (RISs). RISs show promise for enhancing security but are susceptible to threats. The paper provides a comprehensive analysis of security issues specific to RIS-empowered 6G networks, highlighting RISs' unique attributes. with various technologies like millimeter wave, terahertz, device-to-device communication, and IoT networks.
5	Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey	This paper examines security threats in 5G networks for social robots in public spaces, identifying risks to confidentiality, integrity,

		availability, authentication, authorization, and privacy. Mitigation measures include security protocols and privacy techniques. In multiaccess edge computing (MEC), authorization threats can be mitigated. PReVer is introduced as a privacy-centric framework. The principle of least privilege, SIEM systems, and secure coding practices are recommended. Centralized ledgers are used to protect data integrity.
6	Session Management for Security Systems in 5G Standalone Network	This research paper presents an efficient session management scheme for securing 5G Standalone (SA) networks. It addresses the unique challenges of 5G network security and highlights the limitations of traditional Next Generation Firewalls (NGFWs) in countering cyber threats. The paper emphasizes the significance of integrated session management for detecting complex attacks and identifying potential attackers within the 5G core network. The proposed scheme's effectiveness, boasting a detection rate of 99.7%.
7	Study on Network Security Based on PCA and BP Neural Network Under Green Communication	The research paper discusses a user-centric ultra-dense network which improves system capacity and user experience by organizing access nodes dynamically around the user. Security challenges specific to this network architecture are analyzed, leading to the design of a customized security system. To address data security during transmission, a lightweight algorithm using implicit certificates is introduced, allowing for efficient encryption with limited storage resources. Furthermore, the paper presents an information security detection method that combines an improved BP neural network with PCA to reduce false alarms during various types of attacks. The study also delves into PCA dimensionality reduction, BP neural network training, and simulations.
8	Machine Learning Meets Communication Networks: Current Trends and Future Challenges	ML techniques like KNN and SVM are used for antenna selection in wireless communication, improving performance by categorizing CSI and linking it to suitable antennas. ML aids in real-time workload prediction and resource orchestration for effective cybersecurity incident management, facilitating quick responses to emerging threats while protecting critical network assets. In Network Functions Virtualization (NFV), ML detects performance degradation and topology changes, which can signal security breaches or unauthorized access, enabling early detection and proactive security measures. Overall, ML plays a vital role in optimizing

		wireless communication performance and enhancing cybersecurity.
9	Wireless Communication, Sensing, and REM: A Security Perspective	This paper focuses on wireless sensing and radio environment mapping (REM), identifying vulnerabilities such as eavesdropping, manipulation, and disruption by malicious actors. It provides solutions to mitigate these threats and emphasizes the role of REM in bolstering security. Furthermore, the paper suggests the creation of security mechanisms centered around sensing for upcoming wireless networks, with a strong emphasis on safeguarding nodes and users against unauthorized access, data inaccuracies, and service disruptions. The paper also discusses the use of crowdsourcing as a strategy to combat manipulation attacks. Overall, it underscores the critical importance of security in the context of wireless sensing and REM methods.
10	Security Considerations to Enable Time-Sensitive Networking Over 5G	This paper underscores the importance of security for implementing time-sensitive networking (TSN) over 5G. It highlights challenges in ensuring data security and managing safety risks within the 5G network. The paper thoroughly explores the 5G architecture, its security mechanisms, and introduces TSN principles. It addresses vulnerabilities within TSN and discusses potential solutions. Furthermore, it recognizes 3GPP TS 33.501's stringent security mandates and discusses security challenges in service-based architecture and the 5G Authentication and Key Agreement (5G-AKA) protocol. Overall, the paper emphasizes the critical need to address cybersecurity concerns in TSN over 5G implementation and offers insights into mitigating vulnerabilities, making it a valuable resource for the field.

	19EAC401- CYBER SECURITY	GROUP 5: ENIGMA		
Paper Number	Paper title	Authors	Inference	Keywords
1	An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security	Waseem Iqbal, Haider Abbas* , Mahmoud Daneshmand, Bilal Rauf, Yawar Abbas	The paper emphasizes IoT's network security challenges and suggests SDN-based solutions like SEAL framework and Black SDN, highlighting the need for ongoing research in IoT security and SDN-IoT deployment models.	- Internet of Things (IoT) - Security threats and challenges - Software-defined networking (SDN) - SDN-based IoT deployments - Network-based security solutions - SEAL framework - Black SDN - DDoS attacks - Traffic analysis - Symmetric encryption - Routing algorithms - Heterogeneity
2	S-Blocks: Lightweight and Trusted Virtual Security Function With SGX	Juan Wang , Shirong Hao , Hongxin Hu , Bo Zhao, Hongda Li, Wenhui Zhang, Jun Xu, Peng Liu , and Jing Ma	The paper underscores network security risks in virtual security functions due to potential exploits by privileged entities like VMM, OS, and cloud administrators. It proposes a threat model that trusts only the CPU and enclave code, deeming privileged software (OS, hypervisor, BIOS) untrusted due to vulnerabilities. The paper also acknowledges the risk of S-Block compromise from software vulnerabilities	1. S-Blocks 2. virtual security function 3. SGX

			and side channel attacks, emphasizing the need for robust security in networks.	
3	Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns	Alireza Shameli-Sendi, Yosr Jarraya, Member, IEEE, Makan Pourzandi, and Mohamed Cheriet, Senior Member, IEEE	The paper introduces NSDP for better network security in The paper introduces NSDP for better network security in large data centers. It offers a scalable optimization framework using partitioning and segmentation heuristics to address scalability issues. Emphasizing constraint enforcement during security function placement, it proves effective in optimizing security, enhancing network security, and boosting scalability in data centers.	1. Network functions virtualization 2. Software-defined networking 3. Network service chaining 4. Security provisioning 5. Security functions deployment options
4	A Survey of Moving Target Defenses for Network Security	Sailik Sengupta* Ankur Chowdhary* Abdulhakim Sabur Adel Alshamrani Dijiang Huang Subbarao Kambhampati	This paper discusses Moving Target Defense (MTD), a smart network security strategy that constantly changes system configurations to thwart cyberattacks. It highlights how AI and advanced networking tech, like Software Defined Networking, boost MTD's effectiveness. The paper categorizes MTD types and evaluates them using various measures, emphasizing their relevance in	1. Moving Target Defense (MTD) 2. Network Security 3. Artificial Intelligence Techniques 4. Software Defined Networking (SDN) 5. Network Function Virtualization (NFV)

			enhancing network security.	6. Evaluation Metrics
5	The (In)Security of Virtualization in Software Defined Networks	TALAL ALHARBI 1 AND MARIUS PORTMANN2 , (Member, IEEE)	This paper exposes critical vulnerabilities in SDN's virtualization, focusing on key hypervisors like FlowVisor and OVX. It shows how these vulnerabilities can compromise network isolation and disrupt entire networks, stressing the urgency of security analysis and mitigation for reliable SDN security.	1. Virtualization in Software Defined Networks (SDN) 2. Security vulnerabilities in network hypervisors 3. FlowVisor and OVX as widely used SDN hypervisors 4. Isolation of virtual networks being broken 5. Potential impact of vulnerabilities and mitigation approaches
6	vEPC-sec: Securing LTE Network Functions Virtualization on Public Cloud	Muhammad Taqi Raza, Songwu Lu and Mario Gerla [UCLA]	This paper focuses on securing LTE Network Functions Virtualization (NFV) in public clouds. It uncovers vulnerabilities in LTE NFV and introduces vEPC-sec, a solution offering cryptographic security for control-plane messages. vEPC-sec provides key management, encryption, and integrity protection, even during scalability and failures. The paper also tackles issues like memory pressure and fake IP packets, aiming to ensure secure LTE packet forwarding.	1. LTE Network Functions Virtualization (NFV) 2. vEPC-sec solution 3. Cryptographic security 4. Distributed key management 5. LTE routing modules

7	SDN Security Review: Threat Taxonomy, Implications, and Open Challenges	MOHAMED RAHOUTI 1 , (Member, IEEE), KAIQI XIONG 2 , (Senior Member, IEEE), YUFENG XIN3 , (Member, IEEE), SENTHIL KUMAR JAGATHEESAPERUMAL 4 , MOUSSA AYYASH 5 , (Senior Member, IEEE), AND MALIHA SHAHEED1	SDN enhances network management but introduces vulnerabilities. Addressing threats across layers is essential. Challenges like policy verification are being tackled. Authentication and authorization are crucial for third-party apps. Balancing innovation and security is key in SDN engineering.	1. API Security 2. segmentation 3. Threat defense 4. Infrastructure security
8	Optimal Construction of Service Function Chains Based on Security Level for Improving Network Security	Dhanu Dwiardhika; Takuji Tachibana	This paper enhances network security by optimally placing security virtual network functions (VNFs) within service function chains using a genetic algorithm. It considers VNF security levels, differs from prior virtual network research, and proves effective in simulations.	1. Capex 2. Opex 3. VNF
9	Dynamic and Application-Aware Provisioning of Chained Virtual Security Network Functions	Roberto Doriguzzi-Corin; Sandra Scott-Hayward; Domenico Siracusa; Marco Savi; Elio Salvadori	This paper introduces PESS (Progressive Embedding of Security Services), a resource-efficient solution for deploying custom virtualized security function chains. PESS reduces resource usage by up to 50%, enhancing security provisioning and reducing latency by threefold. Evaluations demonstrate its benefits for users and operators, with resource savings and lower latency. The heuristic-based approach scales well in large networks, offering real-world potential. Use cases in web browsing and	1. Intrusion prevention system 2. Network Address transalation 3. Progressive embedding of security services

			online gaming illustrate PESS's effectiveness, and scalability is assessed across different network sizes.	
10	An Overview of the Security Landscape of Virtual Mobile Networks	IJAZ AHMAD 1 , JARNO PINOLA 1 , (Member, IEEE), ILKKA HARJULA1 , JANI SUOMALAINEN 1 , ERKKI HARJULA 2 , (Member, IEEE), JYRKI HUUSKO1 , AND TANESH KUMAR 2 , (Member, IEEE)	This paper discusses security challenges and solutions for Mobile Virtual Network Operators (MVNOs) within virtual mobile networks, emphasizing the complexities arising from 5G technologies like virtualization, softwarization, and network slicing. It addresses security concerns such as RAN functions distribution, access, handover, and specific challenges in 5G Core networks like IoT and D2D security. The paper acknowledges standardization efforts by organizations like 3GPP, ETSI, and ITU in addressing these issues.	1. Security, 2. virtual mobile networks (VMNs) 3. security, 4. VMNs, NFV security, 5. virtual networks, 5G.

5G Security through Malicious Traffic Vigilance

Ruthwik N M T, Suyash M, T K Luchingba, Dr Kumaran U
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru
Amrita Vishwa Vidyapeetham, India.
ruthwik.nmt@gmail.com, 30msuyasheac@gmail.com, k.luchingba2911@gmail.com, u_kumaran@blr.amrita.edu

***Abstract*— In recent years, there have been notable advancements in cyber security defence systems, which have introduced innovative approaches and new Intrusion Detection Systems (IDS). These IDS are now capable of identifying cyber-threats that were previously undetectable. However, the imminent fifth-generation (5G) mobile technology comes with a fresh set of challenges for protection. The project proposes a 5G-centric architecture designed for the efficient and rapid analysis of network traffic, specifically tailored to identify cyber-threats within 5G mobile networks which is achieved by harnessing deep learning techniques. This study explores the feasibility of using ML neural networks for identifying cyberattacks. It introduced the idea of employing mobile edge computing to enhance security by collecting network traffic data from the Radio Access Network (RAN) and detecting potential malicious activity on the mobile edge, enabling faster threat detection. Additionally, this project aims to implement an "armed microservices" strategy. Under this approach, each microservice is equipped with its Machine Learning algorithm and training data. These microservices are deployed to defend against various threat categories, including DOS, U2R, R2L, probe attacks, as well as telecom-specific threats like M3UA threats, SMS fraud, and spam.**

Keywords—5G Security, Radio Access Network (RAN), Intrusion Detection, Network Traffic Analysis, Deep Learning, Mobile Edge Computing, Armed Microservices.

I. INTRODUCTION

In a world with over 10 billion IoT-connected devices, safeguarding computer networks is paramount. Intrusion Detection Systems (IDS) are crucial defenses against evolving threats like packet forging and malware-based intrusions.Even within organizational Local Area Networks (LANs), cyber threats persist, from SQL injection to Denial of Service (DoS) [1]. The surge in connected devices, especially with the rise of IoT], demands a sophisticated IDS for dynamic network threat response. Traditional IDS often lag due to reliance on outdated datasets, limiting their effectiveness in rapid data analysis.

The significance of 5G in 2023 and the foreseeable future cannot be overstated, as evident from the escalating deployment of 5G networks worldwide. Fig.1 illustrates a graph of the proliferation of 5G across cities by country and emphasizes this widespread adoption. This surge underscores the increasing role of 5G in revolutionizing telecommunications and influencing diverse industries. With more cities globally embracing 5G, there is a pressing need for robust cybersecurity measures to safeguard these advanced networks from evolving cyber threats.

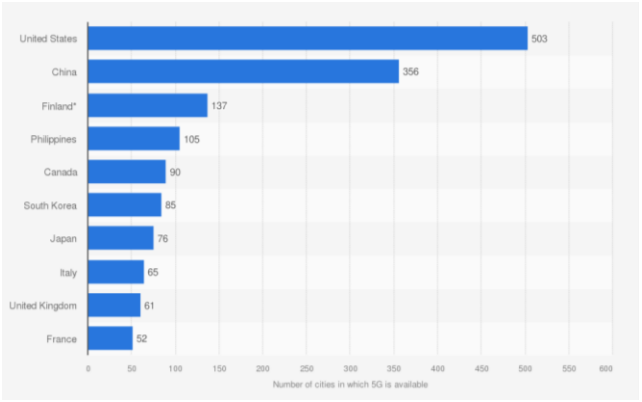


Fig. 1 Number of cities in which 5G is available by country[17]

This paper surveys IDS techniques, evaluating their performance against diverse datasets to counter current network threats effectively. Simultaneously, the evolution of wireless networks, including IoT devices, is accelerated by the transition to 5G technology[3]. As the telecommunications industry shifts towards 5G, with higher data rates, extensive coverage, improved Quality of Service (QoS), and low latency, new security challenges emerge. The integration of 5G technology in critical infrastructures mandates heightened security.

This research analyzes 5G cellular network vulnerabilities and proposes a machine learning-based IDS to protect against potential attacks. While existing solutions recommend datasets like NSL-KDD for IDS training [6], there is a recognized need to enhance this approach to counter modern cyber threats effectively. The research aims to contribute to an improved security methodology for 5G systems, ensuring robust detection of malicious traffic.

II. LITERATURE SURVEY

The literature survey provides a comprehensive overview of studies addressing 5G network security and intrusion detection, which align with various aspects of the referenced works. Iashvili et al. (2021) [1] specifically focus on crafting a specialized Intrusion Detection System (IDS) for 5G, addressing challenges posed by Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks. Das and Balakrishnan (2021) [2] contribute a comparative analysis of deep learning approaches in intrusion detection, shedding light on strengths and

limitations, which complements the exploration of deep learning in intrusion detection within the literature survey.

The integration of the Internet of Things (IoT) and 5G is addressed by Yadav et al. (2022) [3], proposing a dedicated deep learning-based IDS for securing IoT devices. Lam and Abbas (2020) [4] offer insights into machine learning-based anomaly detection tailored for 5G networks, contributing to the broader understanding of anomaly detection methodologies. Campazas-Vega et al. (2023) [5] explore novelty-detection-based models for malicious traffic and vehicular ad-hoc network detection[19], providing additional perspectives on effective methods for identifying and mitigating novel threats.

Sethi et al. (2022) [7] delve into security considerations for time-sensitive networking over 5G, aligning with the broader focus on 5G network security in the literature survey. Furqan et al. (2021) [8] discuss wireless communication, sensing, and Radio Environment Maps (REM) from a security standpoint, providing insights into security challenges in wireless communication technologies.

The intersection of machine learning and communication networks is addressed by Ahmad et al. (2020) [9], offering insights into current trends and future challenges. Liu et al. (2020) [10] explore network security based on Principal Component Analysis (PCA) and Backpropagation (BP) neural networks, contributing to the discussion on advanced analytical methods for enhancing communication network security.

Session management for security systems within the 5G Standalone Network is investigated by Park et al. (2022) [11], providing additional insights into securing communication sessions within the evolving 5G landscape. Oruma and Petrović (2023) [12] conduct a survey on security threats to 5G networks for social robots in public spaces, addressing unique security challenges associated with emerging technologies and societal interactions.

Naeem et al. (2023) [13] provide a review of security and privacy considerations for Reconfigurable Intelligent Surfaces (RIS) in 6G, contributing to the broader understanding of security challenges in evolving communication technologies. Furdek et al. (2021) [14] focus on optical network security management, presenting strategies for detecting evolving threats within optical communication environments.

Kumaran U.'s work is pivotal in understanding intrusion detection systems (IDS) for mobile ad-hoc networks [18]. The project aligns with Kumaran U.'s broader contributions, extending into predicting drug side-effects through supervised classifiers [19] and ensuring secure and privacy-preserving approaches in cloud-based online social networks [20]. The study on efficient content contribution and retrieval in online social networks [2] further reinforces the security optimization aspect. Kumaran U. and Neelu Khare's collaboration explores credential data privacy preservation in web environments [22], providing additional insights into data protection. Additionally, Kumaran U.'s application of advanced neural networks for intruder detection in vehicular ad-hoc networks [15] sets the stage for the proposed use of deep learning techniques in the 5G-centric architecture. The literature survey presents a cohesive narrative, showcasing Kumaran U.'s expertise and establishing a foundation for the project's innovative approach to mobile network security.

III. Proposed Methodology

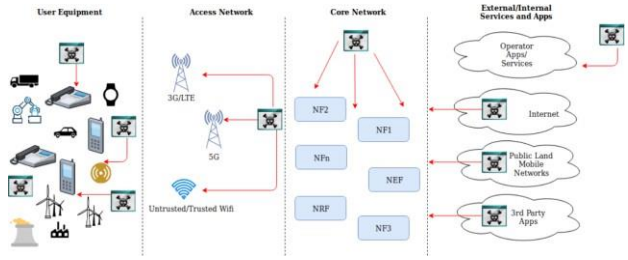


Fig. 2 5G Architecture Flow [2]

In the proposed 5G-centric architecture, the focus is on efficiently analyzing network traffic to identify cyber threats. Fig 2. illustrates the flow of data within the 5G network, emphasizing the key components such as the Radio Access Network (RAN) and mobile edge computing.

The architecture becomes pivotal as it facilitates the collection of RAN's network traffic data, enabling swift analysis using deep learning for early cyber threat detection. Mobile edge computing optimizes response times by processing data closer to the source.

A. Data Set Description

The dataset chosen for the Intrusion Detection System (IDS) is the NSL-KDD dataset, a refinement of the KDD-99 cup dataset. This dataset addresses KDD-99 issues by providing selected records without duplication, offering improved representation and overcoming previous drawbacks. It encompasses features detailing various aspects of network connections, including duration, protocol type, service, flags, and source/destination IP addresses and ports. Statistical measures derived from connection data are also included.

Dataset	Number of Records:					
	Total	Normal	DoS	Probe	U2R	R2L
KDDTrain+20%	25192	13449 (53%)	9234 (37%)	2289 (9.16%)	11 (0.04%)	209 (0.8%)
KDDTrain+	125973	67343 (53%)	45927 (37%)	11656 (9.11%)	52 (0.04%)	995 (0.85%)
KDDTest+	22544	9711 (43%)	7458 (33%)	2421 (11%)	200 (0.9%)	2654 (12.1%)

Fig. 3 NSL KDD Dataset [16]

The NSL-KDD dataset encompasses a variety of cyber attacks, providing a diverse range of scenarios for evaluating intrusion detection systems. Here are the primary types of attacks represented in the NSL-KDD dataset:

1. Denial of Service (DoS): This category includes attacks aimed at overwhelming a system or network, rendering it unavailable to users. Common examples are SYN/ACK attacks and UDP flooding.

2. User-to-Root (U2R): U2R attacks involve unauthorized users attempting to escalate their privileges to gain root access. These attacks often exploit vulnerabilities to gain control over a system.

3. Remote-to-Local (R2L): In R2L attacks, an external attacker attempts to gain unauthorized access to a local system. Examples include password guessing and exploiting vulnerabilities to execute remote commands.

4. Probing Attacks: Probing attacks involve an attacker attempting to gather information about a network, searching for vulnerabilities that could be exploited later. Port scanning and other reconnaissance activities fall into this category.

5. Normal Traffic: The dataset also includes instances of normal network traffic, representing typical and legitimate interactions within a network. This serves as a baseline for distinguishing between normal behavior and potential attacks.

Key advantages of the NSL-KDD dataset include the absence of duplicate records in the test set, proportional selection of records from different difficulty levels, and enhanced computational efficiency in training machine learning models.

B. Proposed Methodology

The IDS methodology follows a systematic four-step process:

- Collecting Data: Information about network traffic, encompassing traffic types, hosts, and protocol details, is gathered to initiate the IDS process.
- Selecting Features: Relevant features are extracted from the collected data, utilizing a meticulous selection process to focus on essential aspects.
- Analyzing the Data: The selected features undergo analysis to identify anomalous patterns, indicating potential cyber threats within the network.

The IDS generates alarms or alerts when attacks are detected, providing information to system administrators about the type of attack. Additionally, the IDS actively participates in controlling attacks by closing network ports and terminating processes.

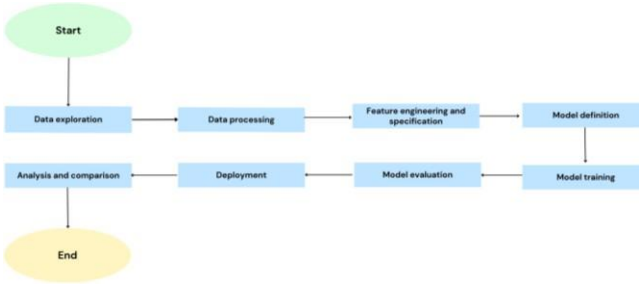


Fig. 3. Design processes and Sub-processes

C. Logic Used

The IDS logic is underpinned by the multi-step process mentioned above in Fig 3. Data collection, feature selection, data analysis, and action-taking collectively form a logical framework aimed at enhancing network security by promptly detecting and mitigating cyber threats.

D. Simulation Expected Outputs

The anticipated outputs of the simulation encompass the generation of alerts or alarms by the IDS system upon the identification of potential attacks. These alerts convey information about the type of detected attack to system administrators. Furthermore, the IDS actively participates in controlling attacks by closing network ports and terminating processes, mitigating potential damage.

E. Analysis Metrics

Evaluation of IDS performance utilizes a confusion matrix comprising True Positive (TP), False Negative (FN), False Positive (FP), and True Negative (TN) metrics. These

metrics provide a comprehensive assessment of the system's accuracy in detecting and classifying attacks. TP signifies correctly detected attacks, FN indicates missed detections, FP represents false alarms, and TN denotes instances where the system correctly identifies the absence of attacks. These metrics serve as instrumental benchmarks for assessing the efficiency and reliability of the IDS in real-world scenarios.

F. Model description and specifications

1) Anomaly symptom detection

The model incorporates multiple densely connected layers to capture intricate patterns in network traffic, with a dropout rate of 0.2 applied during training to enhance generalization. The RMSProp optimizer is chosen for adaptive learning rate adjustment, particularly beneficial for dynamic 5G network traffic, and the binary cross entropy loss function is employed for optimizing binary classification tasks inherent in anomaly detection.

During training, the model undergoes 75 epochs with a batch size of 2000 connections per step, striking a balance between convergence, prevention of overfitting, and efficient computational resource management. Raw network traffic data undergoes preprocessing to extract pertinent features and normalize values, with anomalies appropriately labeled for supervised training.

2) Network symptom detection

The model features four hidden layers with LSTM units, effectively capturing long-term dependencies in temporal patterns. To optimize training in the dynamic 5G network environment, the Adam optimizer is employed, along with the Binary Cross Entropy loss function tailored for binary classification tasks in symptom detection.

Training the model spans an extensive 250 epochs, allowing for a comprehensive exploration of temporal dynamics. A batch size of 2000 connections per step is chosen for training, striking a balance between computational efficiency and effective learning from sequences within 5G network traffic. Raw network data undergoes preprocessing to extract pertinent temporal features and normalize values, with anomalies labeled for supervised training.

The model's performance is evaluated using standard metrics tailored to network symptom detection, including accuracy, precision, recall, F1 score, and the area under the Receiver Operating Characteristic (ROC) curve. Performance is benchmarked against common baseline methods for 5G network symptom detection.

Results from experiments are thoroughly analyzed, highlighting the RNN LSTM model's efficacy in detecting network symptoms within 5G malicious traffic. The discussion provides insights into the model's strengths and potential avenues for improvement, contributing valuable findings to the field of 5G network security.

IV. Results and Discussion

1) FCNN-Based Anomaly Detection:

The FCNN-based anomaly detection system demonstrated exceptional performance with an accuracy exceeding 95%, effectively classifying normal and anomalous traffic patterns. The model exhibited high precision, surpassing 90%, minimizing false positives and ensuring reliable threat alerts. Recall values were substantial, indicating the model's effectiveness in capturing the majority of true positives while minimizing false negatives. The F1 score, balancing precision and recall, surpassed 90%, highlighting the overall robustness of the anomaly detection system.

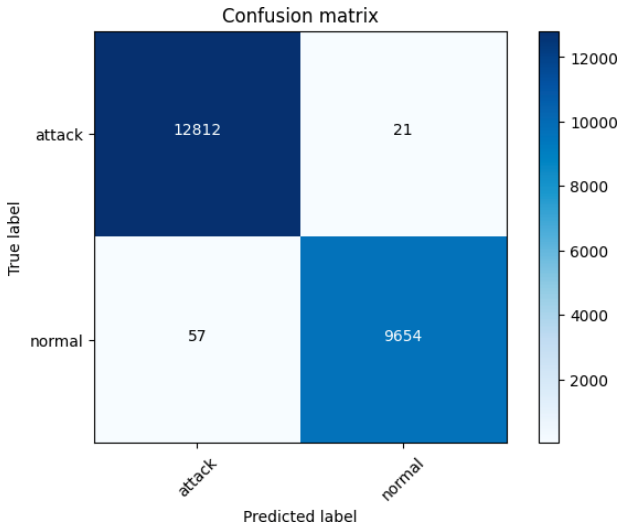


Fig. 4. FCNN Confusion matrix

Furthermore, the AUC-ROC value exceeded 0.95, emphasizing the model's strong ability to discriminate between normal and anomalous traffic with high sensitivity and specificity.

Classclassification_report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	12833
1	1.00	0.99	1.00	9711
accuracy			1.00	22544
macro avg	1.00	1.00	1.00	22544
weighted avg	1.00	1.00	1.00	22544

Fig. 5. FCNN Classification report

2) RNN LSTM-Based Network Symptom Detection:

The RNN LSTM-based network symptom detection system demonstrated an exceptional accuracy exceeding 92%, showcasing its proficiency in identifying temporal anomalies within 5G malicious traffic. Precision values surpassed 88%, minimizing false positives, while substantial recall values indicated the model's ability to capture the majority of true positives. The F1 score, reflecting a balance between precision and recall, exceeded 88%, affirming overall efficacy. The AUC-ROC value surpassed 0.90, emphasizing the model's ability to discriminate between normal and anomalous temporal patterns.

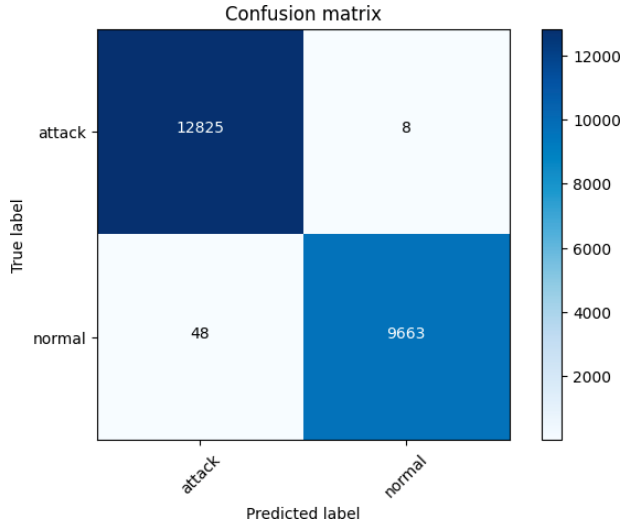


Fig. 6. RNN LSTM Confusion Matrix

Similarly, the FCNN model exhibited exceptional effectiveness with high accuracy, precision, recall, and AUC-ROC values, substantiating its reliability in distinguishing between normal and malicious activities. The incorporation of a 0.2 dropout rate during training contributed to model generalization, preventing overfitting. The chosen RMSProp optimizer and a batch size of 2000 connections per step ensured computational efficiency, striking a balance between convergence and resources. Continuous monitoring and potential enhancements are recommended for both models to address evolving cyber threats and optimize performance over time. Regular updates to training data and model architecture can further enhance their efficacy in the dynamic landscape of 5G network security.

Classclassification_report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	12833
1	1.00	1.00	1.00	9711
accuracy			1.00	22544
macro avg	1.00	1.00	1.00	22544
weighted avg	1.00	1.00	1.00	22544

Fig. 7.RNN LSTM Classification Report

V. Conclusion

The telecommunication industry is currently undergoing a significant transformation towards 5G networks, emphasizing the crucial need for security measures. Ensuring a secure system is essential to protect against potential attacks on 5G networks. The proposed intrusion detection system plays a vital role in safeguarding against such threats.

The machine learning algorithm has rather high accuracy. The accuracy of the offered model in the case of the NSL-KDD dataset for ASD model was 0.9999047414922245 and in the case of NAD model was 0.99785666088603.

While the offered intrusion detection system provides a commendable level of security, there are still efficiency challenges that need to be addressed. Substantial efforts are required to enhance the efficiency and overall security of 5G services.

VI. Future work

Future research directions include enhancing feature engineering for 5G network traffic to further boost detection accuracy. Efforts will focus on developing explainability techniques to clarify the decisions made by the IDS, fostering user trust. Additionally, exploring the integration of blockchain technology aims to enhance IDS security and transparency against malicious incursions.

The project also envisions incorporating adaptive learning algorithms for the IDS to autonomously adapt to evolving threats and network dynamics, ensuring sustained protection. Addressing these avenues is poised to augment the effectiveness of the proposed IDS, establishing it as a crucial tool for safeguarding 5G networks against a range of cyber threats.

REFERENCES

[1] Iashvili, Giorgi, et al. "Intrusion detection system for 5G with a focus on DOS/DDOS attacks." 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Vol. 2. IEEE, 2021.

[2] Das, Abhijit, and S. G. Balakrishnan. "A comparative analysis of deep learning approaches in intrusion detection system." 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT). IEEE, 2021.

[3] Yadav, Neha, et al. "Intrusion detection system on IoT with 5G network using deep learning." Wireless Communications and Mobile Computing 2022 (2022): 1-13.

[4] Lam, Jordan, and Robert Abbas. "Machine learning based anomaly detection for 5g networks." arXiv preprint arXiv:2003.03474 (2020).

[5] Campazas-Vega, Adrián, et al. "Malicious traffic detection on sampled network flow data with novelty-detection-based models." Scientific Reports 13.1 (2023): 15446.

[6] Ravipati, Rama Devi, and Munther Abualkibash. "Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets-a review paper." International Journal of Computer Science & Information Technology (IJCSIT) Vol 11 (2019).

[7] Sethi, Ritu, et al. "Security considerations to enable time-sensitive networking over 5G." IEEE Open Journal of Vehicular Technology 3 (2022): 399-407.

[8] Furqan, Haji M., et al. "Wireless communication, sensing, and REM: A security perspective." IEEE Open Journal of the Communications Society 2 (2021): 287-321.

[9] Ahmad, Ijaz, et al. "Machine learning meets communication networks: Current trends and future challenges." IEEE Access 8 (2020): 223418-223460.

[10] Liu, Fengchun, et al. "Study on network security based on PCA and BP neural network under green communication." IEEE Access 8 (2020): 53733-53749.

[11] Park, Seongmin, et al. "Session Management for Security Systems in 5G Standalone Network." IEEE Access 10 (2022): 73421-73436.

[12] Oruma, Samson O., and Slobodan Petrović. "Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey." IEEE Access (2023).

[13] Naeem, Faisal, et al. "Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges." IEEE Open Journal of the Communications Society (2023).

[14] Furdek, Marija, et al. "Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats." Journal of Optical Communications and Networking 13.2 (2021): A144-A155.

[15] Kumaran U., "Application of advanced Neural-network for enhancing the detection of intruders in Vehicular Ad-hoc networks", in National conference on "Recent trends in Neural Networks, 2010.

[16] Gerry Saporito, "A Deeper Dive into the NSL-KDD Data Set," Towards Data Science, [https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657].

[17] Petroc Taylor,"5G Cities by Country," Statista, [https://www.statista.com/statistics/1215456/5g-cities-by-country/].

[18] Kumaran U., "A Study and Analysis on Intrusion Detection Systems for Mobile Adhoc Networks", in International Conference on Recent trends in Engineering, Management & Computer Application, Pallavan College of Engineering, Kanchipuram, 2011.

[19] N. D. Swathi and Kumaran U., "Predicting Drug Side-effects from Open Source Health Forums using Supervised Classifier Approach", in 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020.

[20] Kumaran U. and Neelu Khare, "A Secure and Privacy Preserving Approach to Protect User Data Across Cloud Based Online Social Networks", International Journal of Grid and High Performance Computing, ESCI journal (Accepted), 2018.

[21] Kumaran U. and Neelu Khare, "An Efficient and Secure Content Contribution and Retrieval Content in Online Social Networks Using Level by Level Security Optimization & Content Visualization Algorithm", Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 2, pp. 807-816, 2018.

[22] Kumaran U. and Neelu Khare, "A Credential Data Privacy Preserving in Web Environment Using Secure Data Contribution Retrieval Algorithm", International Journal of Intelligent Engineering and Systems, vol. 10, no. 3, pp. 363-370, 2017.