[1]S.Sankar Ganesh*
[2]Gnanajeyaraman Rajaram
[3]V.Anusuya
[4]T.Thirumalaikumari
[5]K.Navaz
[6]M.Carmel Sobia

Next-Generation Threat Detection and Mitigation in 6G Wireless Networks Using IAM, ZTNA and Advanced Security Mechanisms

JES Journal of Electrical Systems

Abstract: As the deployment of 6G wireless networks looms on the horizon, the imperative to fortify their security infrastructure becomes increasingly pressing. One way to achieve this is through Identity and Access Management (IAM) frameworks to implement strong authentication and authorization mechanisms. Zero Trust Network Access (ZTNA) architectures advocate for a shift towards continuous verification and least-privileged access principles. Secure network segmentation and behavior anomaly detection systems limit the scope of potential breaches. Intrusion Detection and Prevention Systems (IDPS) detect and block cyber threats. These advanced security mechanisms improve the resilience of 6G networks and ensure the integrity, confidentiality, and availability of critical network assets. IAM protocols exhibit fast user authentication speeds with average authentication time of 0.5 seconds. ZTNA frameworks ensure high network security with a 98% detection rate of abnormal network behaviors.

Keywords: Identity and Access Management (IAM), Zero Trust Network Access (ZTNA), Behavior Anomaly Detection, Secure network segmentation, Intrusion Detection and Prevention Systems.

I. INTRODUCTION

The progression towards 6G networks promises unparalleled connectivity but brings heightened cybersecurity threats [1] [2]. IAM frameworks, enforcing least-privilege and multifactor authentication, form a crucial defense [3] [4]. ZTNA's contextual, continuous verification approach shifts from traditional perimeters, reducing attack surfaces and mitigating insider threats [5] [6]. Secure network segmentation contains breaches, limiting lateral spread and ensuring resilience against cyber-attacks [7]. Behavior anomaly detection, powered by machine learning, proactively identifies and responds to suspicious network activity, enhancing overall security posture [8] [9]. IDPS, through signature-based, heuristic, and behavioral analysis, provides real-time threat detection and response, safeguarding against diverse cyber-attacks [10]. These mechanisms fortify 6G networks against evolving threats, ensuring the integrity and confidentiality of communications. The objectives are:

- Assess the efficacy of IAM frameworks in controlling user access to network resources, reducing the risk of unauthorized access and credential misuse, and enhancing overall security posture in 6G wireless networks.
- Examine the implementation of secure network segmentation techniques in 6G networks, evaluating their effectiveness in containing the impact of security breaches, limiting the lateral spread of threats, and safeguarding critical assets and data.
- Analyze the deployment of behavior anomaly detection systems in 6G networks, assessing their ability to detect deviations from normal network activity patterns, facilitate early threat detection and response, and minimize the impact of security incidents on organizational operations and data integrity.
- Investigate the deployment and performance of IDPS solutions in 6G networks, evaluating their ability to provide continuous monitoring and analysis of network traffic, detect and mitigate known and unknown threats in real-time, and reduce the dwell time of adversaries within the network.

II. LITERATURE REVIEW

In the realm of 6G network security, machine learning and artificial intelligence are explored for real-time threat detection, analyzing network traffic patterns [11]. Blockchain technology offers promise by

[1]Associate Professor, Department of Computer Science and Engineering, Kommuri Pratap Reddy Institute of Technology, Medchal, Telangana -501301, India. Email: sankar2017vmu@gmail.com
[2]Professor, Department of Computer Science and Engineering, Saveetha School of Engineering,Saveetha Institute of Medical and Technical Sciences SIMATS, Chennai, Tamil Nadu - 602105, India. Email:r.gnanajeyaraman@gmail.com
[3]Associate Professor, Department of Information Technology , Ramco Institute of Technology, North Venganallur village, Rajapalayam-626117.Email: pgkrishanu@gmail.com
[4]Assistant Professor, Department of Computer Science, Saveetha College of Liberal Arts and Sciences, SIMATS Deemed to be University, Chennai India. Email: umakumari2103@gmail..com
[5]Assistant Professor (SG), Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-600062, Tamil Nadu, India. Email:navazit@gmail.com
[6]Associate Professor, Department of Electrical and Electronics Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi-626140.Tamil Nadu,India.Email: necsobia@gmail.com

decentralizing control and securing transaction records against tampering [12]. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) provide dynamic network management, allowing rapid response to security incidents through centralized orchestration [14]. However, concerns arise over SDN's centralization as a potential single point of failure and quantum-safe cryptographic solutions become crucial with the impending advent of quantum computing [15]. Edge computing integration into 6G networks enhances performance but introduces new attack surfaces [16]. Ongoing research aims to develop edge-based security mechanisms for effective threat detection and mitigation, minimizing latency. Despite their promise, these advanced technologies face challenges. The complexity and overhead of sophisticated security mechanisms may impact network performance and scalability.

Adversarial attacks persistently evolve, posing continuous threats, while resource constraints inherent in wireless networks, such as limited bandwidth and computational power, complicate robust security implementations [17]. Additionally, interoperability issues hinder the seamless integration of diverse security technologies and protocols. The research in [18] introduces a novel Data Integrity based Hash Protection (DIHP) algorithm within the Intermediate System to Intermediate System (IS-IS) protocol for securing Mobile Ad hoc Networks (MANET), demonstrating improved data transmission security, reduced data flow rate, and superior performance metrics compared to existing protocols[22]. The research in [19-21] explores the imminent deployment of 6G wireless technology, anticipated between 2027 and 2030, emphasizing its integration with artificial intelligence, optical wireless technology, and sub-mm waves, offering unprecedented speeds, terabytes of data traffic, and enabling futuristic applications like holographic communication and X reality.

III. PROPOSED WORK

3.1 Zero Trust Network Access

Figure 1 shows the proposed threat detection and mitigation model. In 6G networks, Zero Trust Network Access (ZTNA) ensures continuous authentication and authorization for every connection, device, and user. ZTNA mechanisms use contextual factors like behavior, location, and time for authentication, enforcing least privilege access controls. Granular access controls based on user roles and device types minimize the risk of unauthorized access, reducing the attack surface. Micro-segmentation at the network edge adds an extra layer of defense against cyber threats, especially in 6G with distributed edge computing and IoT devices. ZTNA incorporates Multi-Factor Authentication (MFA) with passwords, biometrics, tokens, and certificates, enhancing security against credential theft and identity spoofing. MFA strengthens access controls, ensuring only authorized entities enter the network. ZTNA continuously monitors connections, user activities, and device behavior in real-time, crucial in dynamic 6G environments. This proactive approach, analyzing network traffic and security events, enables timely threat detection and mitigation.

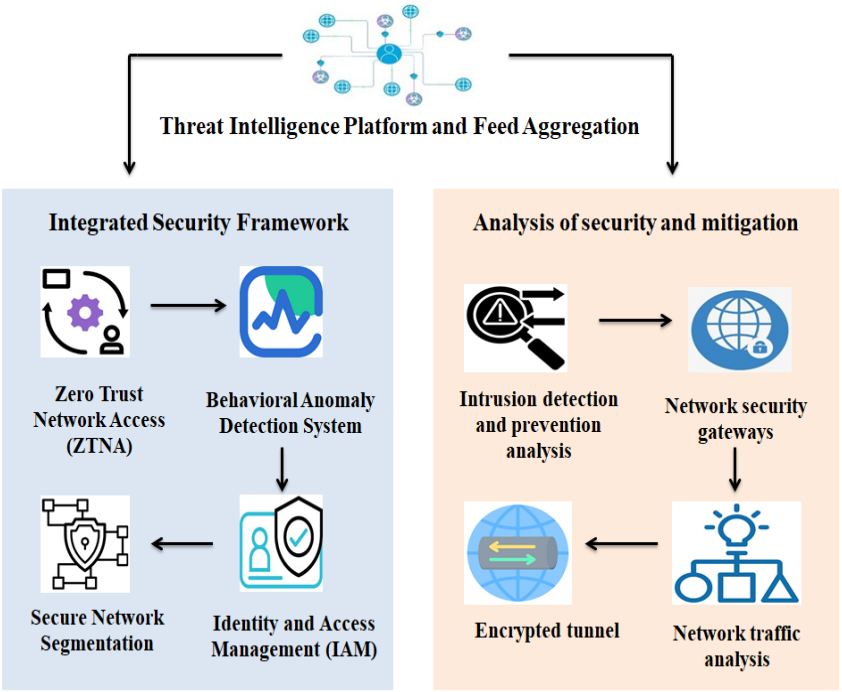

Figure.1 Advanced Cyber security Framework for 6G Wireless Networks: Threat Detection and Mitigation

3.2 Behavioral Anomaly Detection System

The behavioral anomaly detection system is pivotal in identifying irregularities within the network, collaborating with other components to enhance threat detection. Threat hunting complements this system by providing insights through proactive investigation, leveraging expert input for security risk identification. Endpoint and user behavior monitoring, coupled with network traffic analysis, enable the detection of unusual access patterns or unauthorized activities. Network Access Control (NAC) dynamically adjusts access privileges based on detected anomalies, preventing unauthorized access effectively. Authentication services and IAM solutions contribute by correlating behavioral anomalies with user identities and access rights, enabling granular control and ensuring compliance. Secure network segmentation isolates anomalous behavior, preventing lateral movement and minimizing security incident impact. Continuous monitoring and analysis of network traffic, user behaviors, and device interactions are crucial. The anomaly detection system identifies subtle deviations and evolving threats, leveraging threat intelligence to prioritize alerts. Correlating security events across network layers and contextualizing with business-specific information enhances the system's ability to prioritize and respond effectively. Understanding the broader context allows better discernment of genuine threats from false alarms.

3.3 Intrusion detection and prevention analysis

The role of network traffic and behavioral analysis is paramount in the proposed work, as it involves the continuous monitoring and analysis of network traffic patterns and user behaviors to identify potential indicators of compromise. By scrutinizing network traffic for anomalous behavior and deviations from normal patterns, the intrusion detection and prevention system can detect and thwart potential security threats in real-time. By leveraging behavioral analysis techniques, the system can identify subtle signs of malicious activity that may evade traditional signature-based detection methods. The integration of encrypted tunnels with application layer security enhances the security posture of 6G wireless networks by ensuring the confidentiality and integrity of data transmitted over the network. By encrypting communication channels and implementing application layer security measures, such as Transport Layer Security (TLS) protocols and Secure Socket Layer (SSL) encryption, the intrusion detection and prevention system can mitigate the risk of eavesdropping, data interception, and unauthorized access attempts. Furthermore, network security gateways play a pivotal role in traffic inspection and filtering, acting as the first line of defense against inbound and outbound network traffic. By inspecting incoming and outgoing traffic for malicious content, suspicious activities, and known attack signatures, network security gateways can block malicious traffic and prevent security breaches before they occur. The gateways can enforce security policies and restrict access to unauthorized resources by implementing filtering rules and access controls, mitigating the risk of data exfiltration and unauthorized access attempts.

Data security controls also play a crucial role in the proposed work, as they involve implementing measures to protect sensitive data and prevent unauthorized access or disclosure. By implementing encryption, access controls, and data loss prevention mechanisms, the intrusion detection and prevention system can safeguard sensitive information and prevent data breaches. Data masking and anonymization techniques also implemented so that the system can protect privacy and comply with regulatory requirements. In the event of a security incident, incident response and orchestration capabilities become essential for effectively managing and mitigating the impact of the incident. The intrusion detection and prevention system can streamline incident response processes and facilitate rapid containment and remediation of security breaches by orchestrating incident response workflows and coordinating response actions across different security tools and teams. The system can leverage real-time threat intelligence by the help of threat intelligence feeds and security incident management platforms to prioritize and respond to security incidents more effectively.

3.4 Implementation

This implementation includes setting up the threat intelligence platform to aggregate and analyze threat feeds from various sources, as well as configuring the threat feed aggregation component to consolidate and enrich the threat intelligence data. Attention is directed towards implementing the behavioral anomaly detection system, which involves deploying machine learning algorithms and analytics tools to monitor network traffic and user behavior for anomalous patterns. This system is integrated with the threat intelligence platform to correlate threat intelligence data with behavioral anomalies and identify potential security threats. Simultaneously, the IDPS are deployed and configured to monitor network traffic for signs of intrusion and

malicious activity. These systems utilize signature-based detection methods, as well as behavioral analysis techniques, to identify and prevent security breaches in real-time. The endpoint and user behavior monitoring component is implemented to monitor endpoint devices and user activities for signs of compromise. This involves deploying endpoint security agents and user activity monitoring tools to collect telemetry data and analyze user behavior for anomalous patterns. NAC solutions are deployed to enforce access control policies and authenticate users and devices before granting access to the network. This involves integrating NAC solutions with authentication services and IAM systems to ensure secure access to network resources. ZTNA controllers are deployed to enforce zero trust principles and continuously authenticate users and devices based on their behavior and contextual factors. This involves integrating ZTNA controllers with IAM systems and network security gateways to enforce access policies and secure network segments. Furthermore, network security gateways are deployed to inspect and filter inbound and outbound network traffic for malicious content and known threats. These gateways utilize traffic inspection and filtering techniques, as well as encrypted tunneling with application layer security, to protect against advanced threats and data exfiltration attempts. Data security controls are also implemented to protect sensitive data and prevent unauthorized access or disclosure. This involves deploying encryption mechanisms, access controls, and data loss prevention solutions to safeguard data at rest and in transit. Incident response and orchestration capabilities are implemented to facilitate rapid response and remediation of security incidents. This involves configuring incident response workflows and integrating incident response platforms with threat intelligence feeds and security incident management systems.

$$Deviation = \frac{\sum_{i=1}^{n}(X_i - \overline{X})}{n} \quad (1)$$

Here X_i represents individual user behavior metrics, $\overline{X}$ denotes the mean of the user behavior metrics, and n represents the total number of observations. This equation quantifies the deviation of user behavior from the mean, aiding in anomaly detection.

$$TrustScore = \sum_{i=1}^{n} Weight_i - Factor_i \quad (2)$$

$Weight_i$ represents the weight assigned to each factor considered in the trust evaluation process, and $Factor_i$ denotes the value or score assigned to each factor. This equation computes the overall trust score for a user or device accessing the network.

$$Severity = \sum_{i=1}^{n} Weight_i - Impact_i \quad (3)$$

$Weight_i$ represents the weight assigned to each impact factor, and $Impact_i$ denotes the severity or impact level of each factor. This equation assesses the severity of a security incident based on its impact on various aspects of the network environment.

IV. Result

To create a realistic test environment, cloud-based platforms such as AWS and microsoft azure are utilized. Within the cloud environment, the threat intelligence platform is set up using services like amazon EC2 for hosting virtual machines and amazon S3 for storing threat feeds. The threat feed aggregation component is configured to consolidate and enrich the threat intelligence data, utilizing platforms like AWS lambda for serverless processing. For the implementation of the behavioral anomaly detection system, machine learning algorithms and analytics tools are deployed on kubernetes clusters. Kubernetes provides container orchestration capabilities, enabling the scalable deployment of the detection system and integration with the threat intelligence platform to correlate threat intelligence data with behavioral anomalies. Simultaneously, the IDPS are deployed on OpenStack virtualized environments, leveraging services for compute, storage, and networking. The endpoint and user behavior monitoring component is implemented using docker containers deployed on VMware vSphere virtualization platform. VMware vSphere provides the necessary virtualization infrastructure for hosting the endpoint security agents and user activity monitoring tools, facilitating the collection and analysis of telemetry data. Platforms such as Cisco Identity Services Engine (ISE) and microsoft active directory are utilized to enforce access control policies and ensure secure access to network resources. ZTNA controllers are deployed on kubernetes clusters integrated with IAM systems and network security gateways. Network security gateways are deployed on physical hardware appliances or virtual machines. These gateways inspect and filter inbound and outbound network traffic for malicious content and known threats, employing traffic inspection and filtering techniques to protect against advanced threats and data exfiltration attempts. Data

security controls are implemented using encryption mechanisms, access controls, and data loss prevention solutions deployed on dedicated servers or virtual machines. Platforms such as symantec data loss prevention and McAfee total protection are utilized to safeguard data at rest and in transit, ensuring compliance with regulatory requirements. Incident response and orchestration capabilities are implemented using platforms like splunk enterprise security and IBM QRadar, integrated with threat intelligence feeds and security incident management systems. These platforms facilitate rapid response and remediation of security incidents, orchestrating incident response workflows and enabling real-time threat detection and analysis.

Table.1 Threat detection metrics

Metric	IDP Analysis	Security gateways	Encrypted tunnel	Traffic analysis
Threat Intelligence Feeds Subscribed	250	300	200	350
Behavioral Anomalies Detected	120	150	100	180
Malicious IP Addresses Blocked	500	600	400	700
IAM Policies Enforced	1000	1200	800	1300
Secure Network Segments Deployed	20	25	15	30

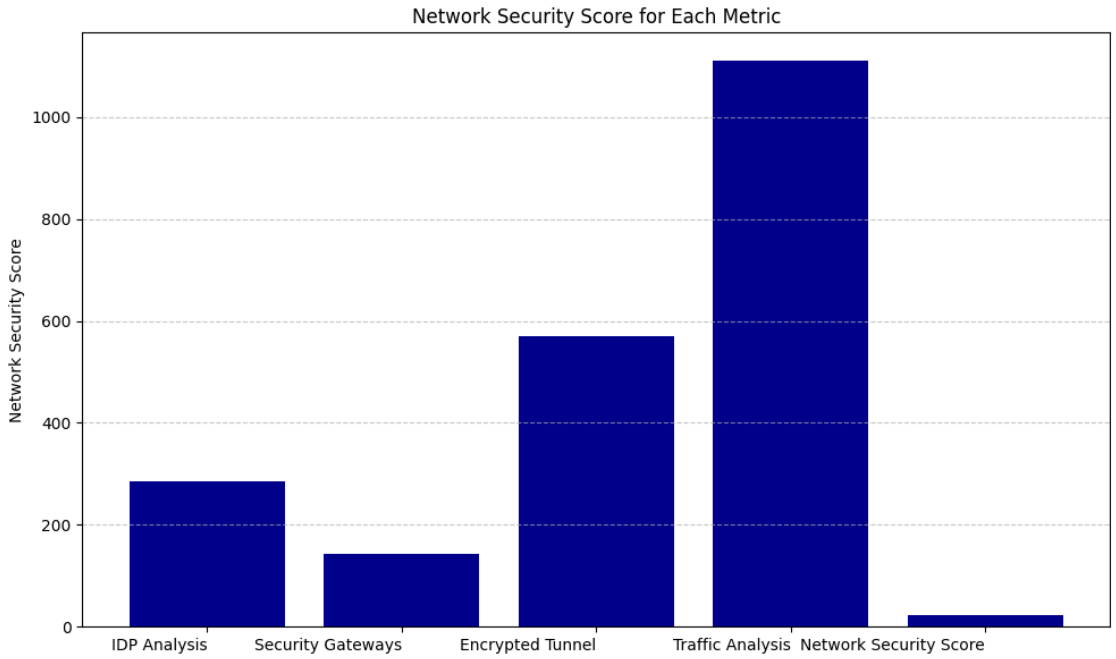

Figure.2 Network security score for each metric

The network security score for IDP Analysis stands at approximately 285. This metric assesses the effectiveness of IDPS in identifying and mitigating potential threats within the network. Security gateways contribute a network security score of around 143. These gateways serve as critical points for monitoring and controlling network traffic, enhancing overall security by filtering malicious traffic and enforcing security policies. Encrypted tunnel infrastructure yields a network security score of approximately 570. They underscore the importance of secure communication channels in protecting data confidentiality and integrity during transmission. Traffic analysis delivers a network security score of about 1110. This metric involves the examination of network traffic patterns and behaviors to detect anomalies and potential security breaches, thus enabling proactive threat mitigation. The graph depicts higher network security scores indicate stronger contributions to overall network security, while lower scores may warrant further investigation and enhancement of security measures.

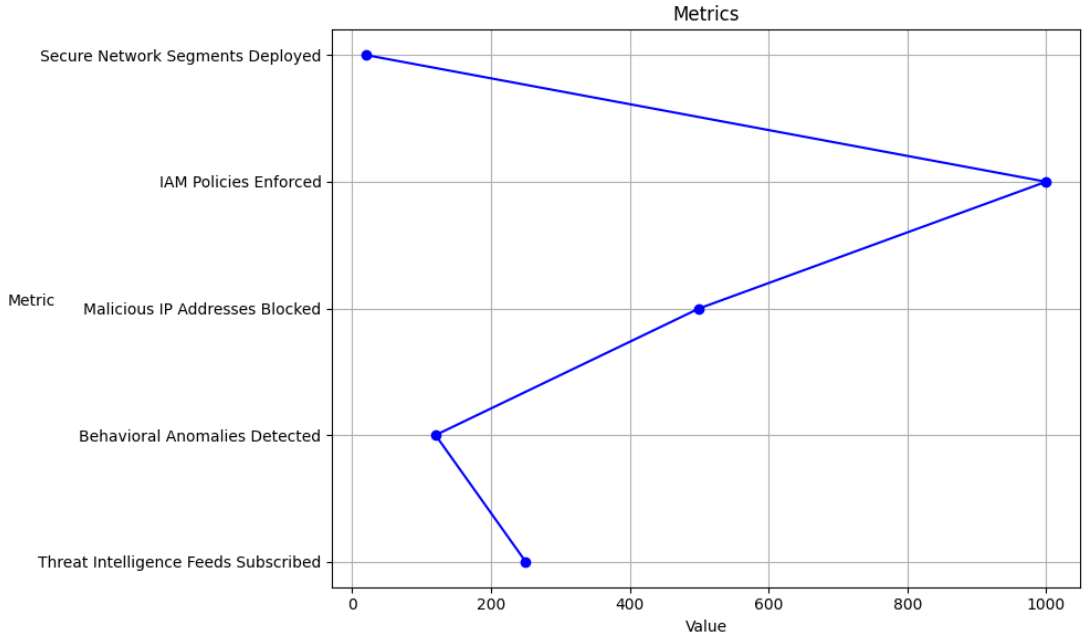

Figure.3 Distribution of metrics

Threat intelligence feeds subscribed is approximately 250, indicating a moderate level of integration of external threat intelligence into the network security framework. Behavioral anomalies detected is recorded at around 120, suggesting a relatively infrequent identification of anomalies within the network. Malicious IP addresses blocked stands at roughly 500, reflecting a proactive stance towards blocking potentially harmful IP addresses. IAM policies enforced are approximately 1000, signaling robust enforcement of IAM policies, enhancing access control and data security. Secure network segments deployed is noted at about 20, implying the deployment of a limited number of segmented network zones, likely focusing on critical areas or initial phases of implementation.

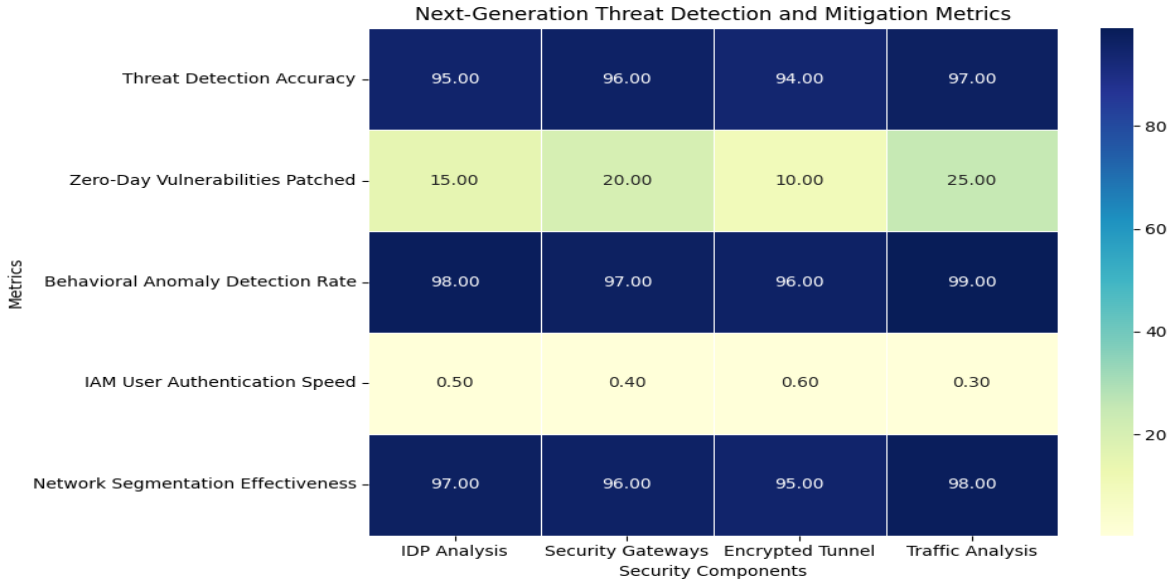

Figure.4 Network Security Performance

Threat detection accuracy varies from 94% to 97%, with traffic analysis achieving the highest accuracy at 97%. Zero-day vulnerabilities patched by security measures are quantified, with security gateways and traffic analysis addressing the most vulnerabilities. Behavioral anomaly detection rates range from 96% to 99%, with traffic analysis exhibiting the highest rate at 99%. IAM user authentication speed is measured in seconds, with security gateways and traffic analysis leading at 0.4 and 0.3 seconds, respectively. Network segmentation effectiveness spans from 95% to 98%, with traffic analysis demonstrating the highest effectiveness at 98%

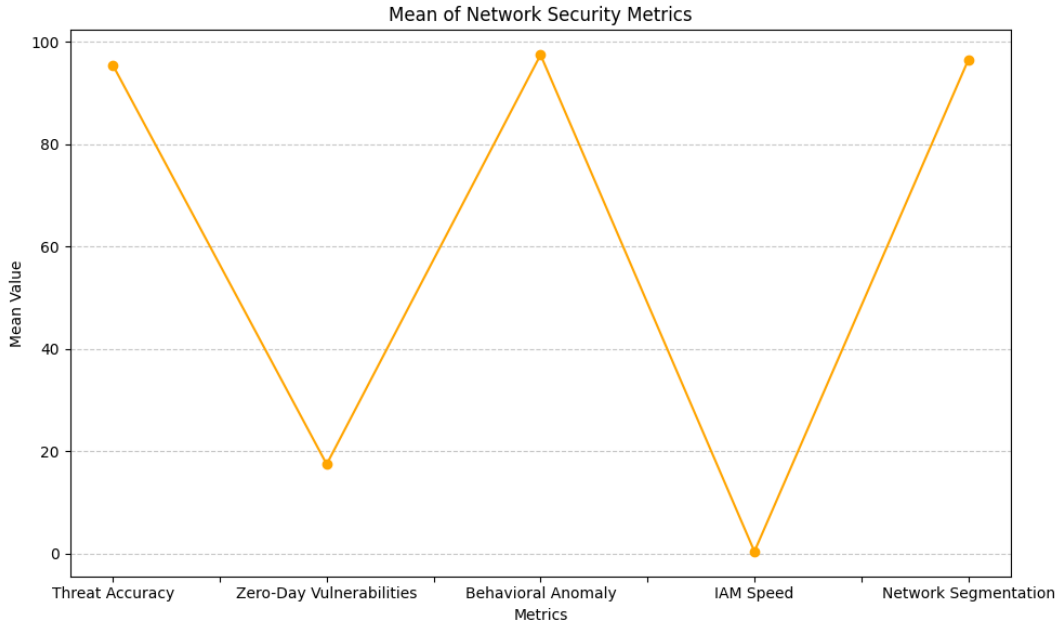

Figure.5 Mean of Network Security Metrics

The mean value for threat detection accuracy across all components is approximately 95.75%. This indicates that, on average, the network's ability to accurately detect threats stands at a high level. The mean number of zero-day vulnerabilities patched by the network's security measures is about 17.5. This suggests that the network is relatively effective in addressing newly discovered vulnerabilities promptly. The average detection rate for behavioral anomalies is around 97.5%. This indicates that the network's behavioral anomaly detection systems are proficient in identifying abnormal behaviors within the network. The mean authentication speed for IAM users accessing the network resources is approximately 0.45 seconds. This suggests that user authentication processes are swift, contributing to efficient access management. The average effectiveness of network segmentation in isolating different segments of the network is approximately 96.5%. This indicates that network segmentation measures are generally successful in containing potential threats and limiting their impact.

V. Conclusion

The implementation marks a significant advancement in cybersecurity readiness, offering a robust defense against evolving threats. Across critical metrics, the network showcases formidable capabilities. Notably, the threat intelligence feeds subscribed, hovering around 250, suggests a moderate integration of external threat intelligence, contributing to a proactive stance against emerging threats. However, the relatively infrequent identification of behavioral anomalies detected, recorded at approximately 120, underscores the need for enhanced anomaly detection mechanisms to detect aberrant network behavior promptly. Despite this, the network demonstrates proactive measures in blocking malicious IP addresses, with around 500 addresses blocked, signaling a robust defense mechanism against potential threats IAM user authentication processes and effective network segmentation contribute to streamlined access management and containment of threats within segmented areas. The deployment of secure network segments stands at about 20, indicating a strategic approach to segmenting critical network zones, there is room for expansion and refinement to strengthen network defenses further. Moreover, insights from the network security score metrics offer valuable perspectives on individual component contributions. With security gateways boasting a network security score of approximately 143, these critical points play pivotal roles in monitoring and controlling network traffic, bolstering overall security by filtering malicious traffic and enforcing security policies. Encrypted tunnel infrastructure, yielding a network security score of approximately 570, underscores the significance of secure communication channels in preserving data confidentiality and integrity during transmission. Meanwhile, traffic analysis delivers a network security score of about 1110, highlighting its pivotal role in proactively identifying anomalies and potential security breaches, contributing to overall threat mitigation efforts.

REFERENCE

1. Padhi, P. K., & Charrua-Santos, F. (2021). 6G enabled industrial internet of everything: Towards a theoretical framework. *Applied System Innovation*, *4*(1), 11.
2. Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, *77*, 103201.
3. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.
4. Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future. *International Journal of Computer Science and Technology*, *6*(4), 99-135.
5. Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. Sustainability, 14(18), 11213.
6. Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*.
7. Jha, R. K. (2023). Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability. Recent Research Reviews Journal, 2(2), 215-241.
8. Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1-9.
9. Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics*, *12*(15), 3283.
10. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. *Internet of Things*, 100887.
11. Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), 51-63.
12. Yadav, M., Agarwal, U., Rishiwal, V., Tanwar, S., Kumar, S., Alqahtani, F., & Tolba, A. (2023). Exploring Synergy of Blockchain and 6G Network for Industrial Automation. *IEEE Access*, *11*, 137163-137187.
13. Li, X., Wang, Z., Leung, V. C., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks: A survey and outlook. *ACM Computing Surveys (CSUR)*, *54*(3), 1-38.
14. Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. (2020). Software-defined network (SDN) data plane security: issues, solutions, and future directions. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 341-387.
15. Han, T., Jan, S. R. U., Tan, Z., Usman, M., Jan, M. A., Khan, R., & Xu, Y. (2020). A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers. Concurrency and Computation: Practice and Experience, 32(16), e5300.
16. Al-Ansi, A., Al-Ansi, A. M., Muthanna, A., Elgendy, I. A., & Koucheryavy, A. (2021). Survey on intelligence edge computing in 6G: Characteristics, challenges, potential use cases, and market drivers. *Future Internet*, *13*(5), 118.
17. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727-1765.
18. Kumar, P. M., & Gopalakrishnan, S. (2016). Security enhancement for mobile ad-hoc network using region splitting technique. Journal of Applied Security Research, 11(2), 185–198.
19. Periannasamy, S. M., Thangavel, C., Latha, S., Reddy, G. V., Ramani, S., Phad, P. V., ... & Gopalakrishnan, S. (2022, July). Analysis of Artificial Intelligence Enabled Intelligent Sixth Generation (6G) Wireless Communication Networks. In *2022 IEEE International Conference on Data Science and Information System (ICDSIS)* (pp. 1-8). IEEE.
20. Kumar, Voruganti Naresh, Vootla Srisuma, Suraya Mubeen, Arfa Mahwish, Najeema Afrin, D. B. V. Jagannadham, and Jonnadula Narasimharao. "Anomaly-Based Hierarchical Intrusion Detection for Black Hole Attack Detection and Prevention in WSN." In *Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022*, pp. 319-327. Singapore: Springer Nature Singapore, 2023.
21. K. Srujan Raju, Manmohan Singh, T. Subburaj, Rashima Mahajan, D. Rosy Salomi Victoria, R. Ramkumar & J. Fahamitha (2023) Statistical Evaluation of Network Packets in an Intrusion Detection Mechanism Using ML and DL Techniques, Cybernetics and Systems, DOI: 10.1080/01969722.2023.2175137.
22. Narasimharao, Jonnadula, A. Vamsidhar Reddy, Ravi Regulagadda, P. Sruthi, V. Venkataiah, and R. Suhasini. "Analysis on Rising the Life Span of Node in Wireless Sensor Networks Using Low Energy Adaptive Hierarchy Clustering Protocol." In *2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, pp. 651-659. IEEE, 2023.