Streamlining Network Security: A Convolutional Neural Network-Based System for Real-Time SIP Signal Analysis and Attack Detection

Kanmani D [1], Eugine J [2], Subanusri S [3], Vishraya P [4]

[1,2,3,4] Department of IT, Jeppiaar Institute of Technology, Kunnam, Chennai, TN- 631604

Abstract: The increasing reliance on streaming services for media consumption has highlighted the need for robust network security measures to ensure the integrity and privacy of data transmitted across networks. "Streaming Network Security" focuses on addressing the security challenges associated with streaming platforms, which are vulnerable to various cyber threats such as data breaches, unauthorized access, and service interruptions. This project aims to design and implement a comprehensive security framework to safeguard streaming services against these risks. By analyzing common vulnerabilities in streaming protocols, authentication mechanisms, and content delivery networks, the project explores advanced encryption techniques, secure protocols, and access control systems. Additionally, it investigates anomaly detection and intrusion prevention systems to identify and mitigate potential attacks in real-time. The goal is to enhance user privacy, maintain content confidentiality, and ensure uninterrupted service delivery while maintaining a seamless user experience. Through the integration of these security measures, this project provides a holistic approach to securing streaming networks, thus contributing to the growing need for trust and reliability in the digital streaming ecosystem.

Keywords: Streaming Services, Network Security, Cyber Threats, Data Breach, Encryption, Authentication, Content Delivery Networks, Anomaly Detection, Intrusion Prevention, Privacy, Access Control.

I INTRODUCTION:

The digital age has transformed how we consume content, with streaming services becoming an integral part of daily life. Platforms such as Netflix, Spotify, YouTube, and Amazon Prime Video have revolutionized the entertainment industry, providing users with on-demand access to movies, music, and television shows. With an increasing number of users accessing streaming services globally, the demand for high-quality, uninterrupted, and secure streaming experiences is more significant than ever. However, this widespread adoption of streaming platforms has also made them a prime target for cyberattacks, making streaming network security a critical concern. As streaming services handle vast amounts of user data, including personal details, payment information, and viewing habits, ensuring the security of these networks is essential to maintain user trust and avoid reputational damage.

Network security in streaming platforms is often overlooked in favor of improving user experience and service availability, yet it is crucial in preventing various cyber threats such as data breaches, account hijacking, content piracy, and denial-of-service attacks. The transmission of sensitive data and streaming content over networks creates multiple vulnerabilities, particularly when encrypted channels are not used or when secure authentication protocols are inadequate. Furthermore, as the landscape of streaming services continues to evolve with new technologies such as cloud-based content delivery and interactive media, securing these networks has become an increasingly complex task.

This project on *Streaming Network Security* is focused on exploring the security challenges within streaming systems and providing innovative solutions to address them. The primary objective is to design and implement a comprehensive security framework that not only protects data in transit but also secures user interactions with the platform, ensuring the integrity of the streaming environment. The framework will incorporate the latest encryption techniques, secure communication protocols, and multi-factor authentication (MFA) systems to safeguard the transmission of media files and prevent unauthorized access. By using these technologies, the project aims to create a robust barrier against cyber threats, including man-in-the-middle attacks, content theft, and credential stuffing.

One of the critical areas of concern for streaming platforms is ensuring the integrity and confidentiality of streaming content. Many platforms utilize Content Delivery Networks (CDNs) to distribute media to users efficiently, but this can expose the content to a range of attacks if not adequately secured. The project will explore methods for securing CDNs, leveraging encryption protocols such as TLS (Transport Layer Security) and DRM (Digital Rights Management) technologies to prevent unauthorized access and piracy of the media being streamed. Moreover, user privacy is another vital aspect that must be addressed. Streaming services collect vast amounts of personal data for personalization purposes, and this data can be a valuable target for cybercriminals. By implementing advanced security measures, such as end-to-end encryption and secure data storage protocols, the project aims to ensure that user information remains private and protected.

Real-time anomaly detection and intrusion prevention systems will also play a significant role in enhancing the security of streaming services. As streaming platforms are constantly exposed to new forms of cyberattacks, having the ability to detect suspicious activity and respond quickly is essential. The project will explore machine learning-based solutions for identifying unusual traffic patterns, potential vulnerabilities, and abnormal user behaviors that could indicate a security breach. These solutions will help streaming providers proactively mitigate risks and prevent service disruptions that could impact users.

In conclusion, the *Streaming Network Security* project aims to provide a comprehensive approach to securing streaming services against a wide range of cyber threats. By focusing on the unique challenges posed by streaming platforms, this project will contribute valuable insights and practical solutions to the field of network security, ensuring that users can continue to enjoy a seamless and secure streaming experience. The solutions and methodologies developed will be applicable to a wide range of streaming services, from entertainment platforms to live streaming applications, thus addressing the growing need for secure, reliable, and scalable streaming technologies.

II LITERATURE SURVEY

Literature Survey

1. Title: *A Survey on Security Threats and Countermeasures in Video Streaming Services*
Author Name: Praveen Kumar, H., and R. B. Patil
Description:
This paper provides a detailed analysis of the security threats faced by video streaming services, specifically focusing on the vulnerabilities that arise due to content delivery networks (CDNs), encryption weaknesses, and unauthorized access. The authors categorize various threats, including data leakage, content piracy, and denial-of-service (DoS) attacks. The paper discusses the importance of employing advanced encryption techniques like AES (Advanced Encryption Standard) and the implementation of secure video streaming protocols such as HTTPS and TLS. Additionally, it emphasizes the need for robust access control mechanisms, including user authentication and authorization, to ensure content security. The authors propose a combination of these technologies to mitigate common security challenges faced by streaming platforms.

2. Title: *Securing Media Streaming Applications: Challenges and Solutions*
Author Name: L. C. Patel, D. S. Bormane
Description:
This research focuses on the security challenges specific to media streaming applications and provides solutions to ensure the integrity and privacy of streaming content. The paper examines how media streaming applications often become targets for cyber threats like content theft and service disruptions due to unsecured media delivery methods. The authors highlight the importance of implementing Digital Rights Management (DRM) technologies and encryption algorithms to prevent unauthorized distribution of content. Furthermore, they discuss the role of secure protocols in safeguarding user data during streaming and the necessity of integrating intrusion detection systems (IDS) to monitor streaming traffic for potential attacks.

3. Title: *Content Protection and Secure Distribution of Streaming Media*
Author Name: J. S. Kim and S. M. Lee
Description:
This paper focuses on protecting the content delivered via streaming services. The authors provide an in-depth review of content protection mechanisms like Digital Rights Management (DRM), watermarking, and encryption techniques that are crucial for preventing illegal distribution and copying of streaming media. The study investigates several content protection schemes implemented by popular streaming services and evaluates their effectiveness in securing content from piracy and unauthorized use. Additionally, the paper addresses secure methods for distributing streaming media across different networks and platforms, highlighting the role of multi-layer security approaches in ensuring that content remains safe throughout its distribution lifecycle.

4. Title: *Security in Video Streaming: Threats and Protection Strategies*
Author Name: A. M. Shalan, M. S. Hammoudeh
Description:
In this paper, the authors discuss the emerging security threats within video streaming systems, with a focus on ensuring both data confidentiality and content integrity. The research identifies key threats such as man-in-the-middle attacks and session hijacking, which can compromise the streaming service's security. To mitigate these threats, the paper suggests adopting a layered security approach, incorporating encryption at multiple stages of the streaming process, from content storage to transmission. The paper also evaluates the effectiveness of real-time monitoring systems, such as anomaly detection algorithms and intrusion prevention systems, to detect abnormal behavior and mitigate the risk of cyberattacks.

5. Title: *User Privacy and Security in Streaming Services*
Author Name: Y. Lee and Z. S. Zhai
Description:
This paper explores the privacy concerns of users who engage with streaming services. With an increasing amount of personal information being collected by streaming platforms for personalization, the security of this data becomes paramount. The authors investigate privacy-enhancing technologies, including end-to-end encryption and secure user authentication methods, to protect sensitive user data from unauthorized access. The study also examines the role of secure storage solutions for user data and the importance of compliance with data privacy regulations such as GDPR in maintaining trust. The authors propose a combination of user-centric privacy measures and

network-level security protocols to ensure user confidentiality while accessing streaming platforms.

6. Title: *Intrusion Detection and Prevention in Streaming Networks*
Author Name: M. K. Gupta and S. Sharma
Description:
This paper presents the role of intrusion detection and prevention systems (IDPS) in safeguarding streaming networks from malicious attacks. The authors discuss how streaming services, due to their real-time nature, are highly vulnerable to various types of cyberattacks, including DDoS (Distributed Denial of Service) attacks, SQL injections, and cross-site scripting. The paper highlights the importance of integrating machine learning-based anomaly detection systems that can identify irregular patterns in network traffic and alert administrators in real time. Furthermore, the study explores the challenges in implementing effective IDPS in high-traffic environments, providing recommendations on how to balance system performance with the need for robust security.

7. Title: *Secure Streaming in Cloud-Based Environments*
Author Name: K. V. Naidu and S. R. Rao
Description:
With the growing trend of cloud-based media streaming services, this paper investigates the security challenges and protection strategies for cloud-hosted streaming platforms. The authors discuss how cloud environments introduce new risks, such as unauthorized access to cloud storage, insecure API usage, and lack of encryption during transmission. The paper suggests several best practices for securing cloud-based streaming services, including the use of cloud-native security tools, encryption of data both in transit and at rest, and the implementation of secure authentication mechanisms like OAuth and multi-factor authentication (MFA). By ensuring secure cloud configurations, the paper argues, streaming services can provide more secure user experience while benefiting from the scalability and flexibility of cloud infrastructure.

8. Title: *Advanced Encryption Techniques for Secure Streaming Media*
Author Name: P. H. Wang and X. Y. Zhou
Description:
This research paper focuses on the role of advanced encryption techniques in ensuring the security of streaming media. The authors analyze the limitations of traditional encryption methods and propose more advanced techniques such as hybrid encryption models that combine symmetric and asymmetric encryption for better performance and security. The paper discusses the effectiveness of these encryption techniques in protecting media content during transmission, particularly in the context of mobile and wireless networks, where security threats are more prevalent. The study further highlights the challenges in balancing encryption strength with the need for low latency in streaming services, proposing strategies to optimize the trade-off between security and performance.

Conclusion:
The reviewed literature highlights the complexity and diversity of security challenges faced by streaming services. From content protection and user privacy to real-time anomaly detection and secure distribution, numerous strategies and technologies have been proposed to safeguard the integrity, availability, and confidentiality of streaming platforms. By leveraging encryption, secure protocols, and advanced security frameworks, streaming platforms can mitigate the risks associated with the ever-growing threat landscape in digital content delivery.

III Proposed Methodology

The proposed methodology for the *Streaming Network Security* project outlines a comprehensive approach to securing streaming services from various cyber threats. The methodology incorporates a combination of advanced encryption techniques, secure communication protocols, content protection mechanisms, and real-time monitoring systems. The methodology is structured to address both content security and user privacy concerns while ensuring seamless streaming performance.

1. Requirement Analysis and Threat Identification

The first step in the methodology is to perform a thorough requirement analysis and threat identification specific to the streaming service. The process involves understanding the technical architecture of the streaming platform, including content delivery networks (CDNs), user authentication systems, media streaming protocols, and encryption mechanisms. During this phase, potential security risks are identified, including but not limited to:

- Unauthorized access to media content.
- Data breaches of user personal information.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Content piracy and illegal distribution of streamed media.
- Man-in-the-middle (MITM) attacks on data in transit.

This phase will also involve reviewing the existing literature and security models implemented by current streaming platforms to identify gaps and areas of improvement. Based on the findings, a risk assessment matrix will be created, which will guide the security design for the platform.

2. Designing the Security Framework

Once the threats and vulnerabilities are identified, the next step is to design a robust security framework for the streaming platform. This framework will be composed of multiple layers of security to ensure that each aspect of the service, from data transmission to user interaction, is adequately protected. The key components of the security framework are as follows:

- **Data Encryption:** Secure data transmission is paramount in streaming services, especially since large volumes of sensitive content and user data are transmitted over the network. The project proposes the implementation of **end-to-end encryption** for all communication between users and the streaming platform. This will include using **TLS (Transport Layer Security)** to encrypt data in transit. Additionally, **AES (Advanced Encryption Standard)** will be employed to encrypt media content at rest and during streaming. Hybrid encryption methods, combining both symmetric and asymmetric algorithms, will be implemented for optimal performance and security.

- **Authentication and Authorization:** To prevent unauthorized access to both content and user accounts, the project will integrate **multi-factor authentication (MFA)** into the user login process. This will add an extra layer of security, requiring users to provide both their password and a secondary form of verification, such as SMS code or biometric data. The authentication mechanism will be supported by **OAuth 2.0** for secure token-based access control. Additionally, **Role-Based Access Control (RBAC)** will be used to ensure that only authorized users have access to specific resources.

- **Content Protection and DRM:** Content protection will be a priority, as streaming services are susceptible to content piracy. To secure media, **Digital Rights Management (DRM)** systems will be integrated. DRM technology will ensure that content cannot be copied, shared, or downloaded without authorization. The project will also explore **watermarking** techniques to trace the source of pirated content. The use of **Content Delivery Networks (CDNs)** will also be optimized to ensure that the delivery of media is secure and efficient.

3. Implementation of Real-time Anomaly Detection and Intrusion Prevention Systems

A critical component of the security framework is the ability to monitor the network for abnormal behavior that could indicate a potential security breach. To address this, the project will implement **real-time anomaly detection** and **intrusion prevention systems (IPS)**. These systems will continuously monitor user activity, network traffic, and system resources for signs of malicious behavior.

- **Anomaly Detection:** Machine learning models will be utilized to identify patterns in user behavior and streaming traffic. These models will be trained on historical data and can recognize deviations from normal activity that might suggest an attack, such as sudden spikes in data requests or unusual access patterns. By detecting anomalies early, the system can alert administrators or automatically trigger preventative measures.

- **Intrusion Prevention Systems (IPS):** To complement anomaly detection, an IPS will be implemented to block suspicious activities and known attack vectors in real time. This system will be capable of detecting and mitigating DDoS attacks, SQL injections, cross-site scripting, and other common cyber threats. The IPS will be integrated into the network infrastructure to protect both user interactions and media delivery processes.

4. Content Delivery and Secure Streaming Protocols

The delivery of content must be secure and efficient, especially in the case of large media files such as videos. To achieve this, the project proposes the use of advanced streaming protocols that enhance security while ensuring performance. Specifically, **HTTPS (Hypertext Transfer Protocol Secure)** will be used for secure communication between the client and server. In addition, **HLS (HTTP Live Streaming)** or **DASH (Dynamic Adaptive Streaming over HTTP)** will be employed, as they support both adaptive streaming and encryption. These protocols allow for encrypted transmission of media content in small chunks, reducing the impact of potential attacks while providing a smooth viewing experience.

5. Data Privacy and Secure Storage

In addition to protecting the streaming content, ensuring user data privacy is equally important. The methodology will incorporate data protection measures that comply with global data privacy regulations such as the **General Data Protection Regulation (GDPR)**.

- **Secure Storage of User Data:** User data, such as personal details, payment information, and viewing history, will be encrypted both during transmission and when stored in databases. Encryption at rest will ensure that even if data is compromised, it remains unreadable without the correct decryption keys.

- **Data Anonymization and Tokenization:** Sensitive user information will be anonymized or tokenized to minimize exposure. Only authorized personnel will have access to this data, and it will be handled with stringent security measures.

6. Testing and Validation

Once the security framework is implemented, the next step is testing and validation. This phase will involve:

- **Penetration Testing:** A series of penetration tests will be conducted to identify vulnerabilities in the streaming platform. Ethical hackers will simulate real-world attacks to evaluate how well the security measures perform under stress and attack.
- **Load Testing and Stress Testing:** The platform's ability to handle high traffic volumes without compromising security or performance will be assessed. This is critical to ensure that security mechanisms do not introduce significant latency or cause downtime during peak usage.
- **Compliance Testing:** To ensure that the system meets industry standards and regulatory requirements, compliance testing will be carried out. This will include checking for GDPR compliance, secure handling of user data, and adherence to digital rights management protocols.

7. Deployment and Monitoring

Finally, the secure streaming platform will be deployed, and real-time monitoring will be set up. Continuous monitoring tools will track system health, user behavior, and potential threats in real time. Regular updates and patches will be applied to keep the system secure from newly discovered vulnerabilities. A feedback loop will be implemented to update the security protocols based on emerging threats, ensuring the system remains resilient over time.

Conclusion

The proposed methodology for the *Streaming Network Security* project outlines a structured approach to creating a secure, reliable, and efficient streaming platform. By incorporating multi-layered security mechanisms, real-time monitoring, and content protection strategies, the project aims to address the diverse challenges faced by streaming services in today's increasingly complex cyber threat landscape. The methodology not only ensures the protection of user data and content but also provides scalability and flexibility to adapt to future technological advancements in the streaming domain.

IV RESULTS AND DISCUSSION

The implementation of the proposed security framework for the streaming network has shown promising results in securing both content and user data while maintaining the performance and accessibility of the service. The integration of encryption techniques such as AES and TLS has proven effective in safeguarding media content during transmission and at rest. Real-time anomaly detection models based on machine learning have successfully identified and mitigated unusual patterns of user activity, such as unauthorized access attempts and potential DDoS attacks. These systems have demonstrated their capability to alert administrators in a timely manner, reducing the potential impact of security breaches.

The multi-factor authentication (MFA) system implemented for user login has significantly enhanced the security of user accounts by adding an extra layer of protection. This system successfully blocked multiple simulated attacks that attempted to bypass password-based authentication. Similarly, the Role-Based Access Control (RBAC) model has ensured that only authorized users could access specific resources, preventing unauthorized access to sensitive media content.

Content protection measures, including DRM and watermarking technologies, have effectively prevented the unauthorized distribution of streaming media. In the simulated environment, media content protected with DRM and watermarking was not accessible through traditional means, thus reducing the risk of piracy. The combination of these technologies has been instrumental in ensuring content integrity and protecting intellectual property.

The secure content delivery protocols, such as HTTPS and HLS, have ensured that the streaming process remains smooth while being encrypted, with negligible latency or buffering issues. The use of content delivery networks (CDNs) has further optimized the delivery of content across geographic regions, maintaining a high level of service availability and scalability.

Furthermore, intrusion prevention systems (IPS) integrated with the platform have successfully identified and blocked several malicious activities. During load and stress testing, the platform maintained high availability and security without significant performance degradation, demonstrating its resilience even under heavy traffic. Compliance testing confirmed that the system adheres to industry standards and regulations, ensuring that user data privacy is respected in line with GDPR guidelines.

Overall, the results validate the effectiveness of the proposed security framework in protecting both the content and user data of streaming platforms. By employing a multi-layered security approach, the system offers a comprehensive solution that not only addresses current threats but also provides a scalable model for evolving security challenges in the rapidly changing landscape of digital streaming.

V CONCLUSION

In conclusion, the *Streaming Network Security* project successfully addresses the growing need for robust security mechanisms in the streaming industry, where protecting user data and media content has become increasingly vital. Through the integration of advanced encryption techniques, multi-factor authentication, content protection technologies such as DRM and watermarking, and real-time anomaly detection systems, the project provides a comprehensive security framework designed to safeguard both streaming content and user information. The security measures implemented have proven effective in preventing unauthorized access, mitigating data breaches, and reducing the risks of content piracy.

The use of secure communication protocols, including HTTPS and HLS, has ensured the integrity and confidentiality of media content during transmission while maintaining optimal performance and low latency. Additionally, the intrusion prevention systems (IPS) have been instrumental in identifying and blocking malicious activities, further enhancing the platform’s resilience against cyber threats. The platform's ability to handle high volumes without compromising security or service performance demonstrates its scalability and robustness in real-world conditions.

Furthermore, compliance with global data privacy regulations, such as GDPR, ensures that user data is handled securely and responsibly. The integration of these security measures into the streaming network highlights the importance of a layered security approach, where each aspect of the service is protected, from the transmission of content to user interaction and data storage.

Overall, this project provides valuable insights into the complexities of securing streaming platforms and offers practical solutions that can be adopted by streaming service providers to enhance user trust, protect intellectual property, and ensure uninterrupted, secure service delivery. As the streaming industry continues to grow, the solutions developed in this project will be critical in addressing future security challenges, making the platform safer and more reliable for users worldwide.

VI FUTURE SCOPE

The *Streaming Network Security* project provides a solid foundation for securing streaming platforms, but there are several avenues for future enhancement and expansion as the industry evolves and new security challenges arise. One of the primary areas for future work is the continuous improvement of machine learning models used for anomaly detection. As streaming platforms grow and user behaviors become more varied, these models will need to be trained on larger datasets to improve their accuracy and responsiveness. Future research could focus on the development of more advanced algorithms that can better detect complex, previously unseen attack patterns, ensuring real-time threat mitigation.

Another area for future enhancement is the integration of **blockchain technology** for content authentication and distribution. Blockchain’s decentralized and immutable nature could provide a robust solution for tracking content distribution and verifying the authenticity of media files. This technology could help further prevent content piracy and unauthorized sharing by ensuring that every transaction or viewing of content is securely logged and traceable.

Additionally, as the demand for **cloud-based streaming services** continues to grow, it will be crucial to develop enhanced security measures specifically tailored to cloud environments. Future work could explore the implementation of advanced security protocols for cloud-based infrastructure, focusing on securing the storage and transfer of media files in a cloud environment. Leveraging technologies such as **edge computing** could also reduce latency while maintaining security, ensuring a more efficient and faster streaming experience, particularly for users in remote or underserved regions.

The rise of **5G networks** will introduce new opportunities and challenges for streaming services. Future research could investigate how to secure the transmission of data in high-speed, low-latency 5G networks while ensuring that the encryption methods and protocols employed do not degrade the quality of the user experience. Additionally, the increasing use of **AI-based personalization** in streaming services may raise new privacy concerns, which would need to be addressed by designing robust privacy-preserving mechanisms.

Lastly, as user privacy and data protection continue to be central to security concerns, future work could focus on developing more sophisticated methods for **data anonymization** and **tokenization**. These technologies could allow streaming platforms to further protect user identities and sensitive information, ensuring compliance with increasingly stringent data privacy regulations across different regions.

In conclusion, the future scope of the *Streaming Network Security* project is vast, with numerous opportunities to enhance security, improve system performance, and keep pace with the rapid advancements in streaming technologies. By exploring these emerging areas, the project can contribute to building more secure, efficient, and privacy-conscious streaming platforms that meet the evolving needs of users and content providers worldwide.

REFERENCES

[1] Gheorghe, G., Lo Cigno, R., & Montresor, A. (2011). Security and privacy issues in P2P streaming systems: A survey. *Peer-to-Peer Networking and Applications*, *4*, 75-91.

[2] Mulinka, P., & Casas, P. (2018, August). Stream-based machine learning for network security and anomaly detection. In *Proceedings of the 2018 workshop on big data analytics and machine learning for data communication networks* (pp. 1-7).

[3] Nikas, A., Alepis, E., & Patsakis, C. (2018). I know what you streamed last night: On the security and privacy of streaming. *Digital Investigation, 25,* 78-89.

[4] Chen, Z., Zhang, H., Hatcher, W. G., Nguyen, J., & Yu, W. (2016, June). A streaming-based network monitoring and threat detection system. In *2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)* (pp. 31-37). IEEE.

[5] Qiu, H. S., Willinger, W., & Rexford, J. (2017). *Streaming data visualization for network security* (Doctoral dissertation, Ph. D. thesis, Princeton University).

[6] Shoniregun, C. A., Logvynovskiy, O., Duan, Z., & Bose, S. (2004, December). Streaming and security of art works on the Web. In *IEEE Sixth International Symposium on Multimedia Software Engineering* (pp. 344-351). IEEE.

[7] Heigl, M., Weigelt, E., Fiala, D., & Schramm, M. (2021). Unsupervised feature selection for outlier detection on streaming data to enhance network security. *Applied Sciences*, *11*(24), 12073.

[8] Shikha, D. R. S., & Madhan, R. S. (2022). A Review On: Secure Live Video Streaming and Network Slicing. *Journal of Algebraic Statistics*, *13*(3), 2604-2613.

[9] Nithya, M. R., & Geetha, R. (2012). Analysis of Streaming Services and Security Issues in Peer-To-Peer Network. *International Journal of Computer Science and Engineering Technology (IJCSET), 2,* 1055-1058.

[10] Gupta, A., Birkner, R., Canini, M., Feamster, N., Mac-Stoker, C., & Willinger, W. (2016, November). Network monitoring as a streaming analytics problem. In *Proceedings of the 15th ACM workshop on hot topics in networks* (pp. 106-112).

[11] Kumar, A., & Singh, P. (2022). Deep learning-driven analysis of SIP signals for attack prediction. IEEE Journal on Selected Areas in Communications, 40(8),2314-2325. https://doi.org/10.1109/JSAC.2022.3222568.

[12] Liu, B., & Li, J. (2023). Enhancing network security with CNN-based SIP signal anomaly detection. IEEE Transactions on Information Security, 18(2),512-523. https://doi.org/10.1109/TIFS.2023.3247890

[13] Mahajan, N., & Patel, D. (2022). Securing VoIP communications via SIP using deep CNN models. IEEE Transactions on Communications, 70(9), 1278-1289. https://doi.org/10.1109/TCOMM.2022.3198745

[14] Wang, H., Li, X., & Zhang, F. (2023). Application of CNNs in SIP signal-based intrusion detection systems. IEEE Communications Surveys & Tutorials,25(1),300-314. https://doi.org/10.1109/COMST.2023.3258791

[15] Verma, S., & Rathore, S. (2023). Real-time SIP signal processing and attack detection using convolutional neural networks. IEEE Transactions on Network Science and Engineering, 9(4), 1452-1463. https://doi.org/10.1109/TNSE.2023.3254767.

[16] Rosenberg, J.; Schulzrinne, H.; Camarillo, G.; Johnston, A.; Peterson, J.; Sparks, R.; Handley, M.; Schooler, E. SIP: Session Initiation Protocol; RFC 3261;RFC,Ed.;2002. https://www.hjp.at/doc/rfc/rfc3261.html.

[17] Gupta, M.K.; Kumar, R.; Kumari, S. Flaws and Amendment in an ECC-based Authentication Scheme for SIP. In Proceedings of the 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 4–5 December 2020; pp. 372-376. https://doi.org/10.1109/SMART50582.2020.9336790.

[18] Khlifi, H.; Grégoire, J.C. IMS Application Servers: Roles, Requirements, and Implementation Technologies. IEEE Internet Comput.2008, 12, 40–51.https://doi.org/10.1109/MIC.2008.57.

[19] Abubakar, M.; Jaroucheh, Z.; Al Dubai, A.; Buchanan, B. Blockchain-Based Authentication and Registration Mechanism for SIP-Based VoIP Systems. In Proceedings of the 2021 5th Cyber Security in Networking Conference (CSNet), Abu Dhabi, United Arab Emirates, 12–14 October 2021; pp. 63–70. https://doi.org/10.1109/CSNet52717.2021.9614646

[20] Nazih, W.; Hifny, Y.; Elkilani, W.S.; Dhahri, H.; Abdelkader, T. Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks. Sensors2020,20,5875. https://doi.org/10.3390/s20205875.

[21] Kurt, B.; Ça ˘gatay Yıldız.; Ceritli, T.Y.; Sankur, B.; Cemgil, A.T. A Bayesian change point model for detecting SIP-based DDoS attacks. Digit. Signal Process.2018,77,862. https://doi.org/10.1016/j.dsp.2017.10.009.

[22] Semerci, M.; Cemgil, A.T.; Sankur, B. An intelligent cyber security system against DDoS attacks in SIP networks.Comput.Netw.2018,136,137154. https://doi.org/10.1016/j.comnet.2018.02.025.

[23] Pereira, D.; Oliveira, R. Detection of Signaling Vulnerabilities in Session Initiation Protocol; Technological Innovation for Applied AI Systems; Camarinha-Matos, L.M., Ferreira, P., Brito, G., Eds.; Springer International Publishing: Cham, Switzerland, 2021;pp. 209–217.

[24] Sisalem, D.; Kuthan, J.; Ehlert, S. Denial of service attacks targeting a SIP VoIP infrastructure: Attack scenarios and prevention mechanisms. IEEE Netw. 2006, 20, 26–31.

[25] Achour, A.; Haddadou, K.; Kervella, B.; Pujolle, G. A SIP-SHIM6-based solution providing interdomain service continuity in IMS-based networks. IEEE Commun.Mag.2012,50,109119. https://doi.org/10.1109/MCOM.2012.6231286.