International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ROBUST AND LIGHTWEIGHT INTRUSION DETECTION MODEL FOR ATTACK CLASSIFICATION IN 5G ENVIRONMENTS

Shammi Wasim, Dr Jameel Ahmad

#1integral university Lucknow, shammi@iul.ac.in

*2 integral university Lucknow, Associate Professor, jameel@iul.ac.in

MCN: IU/R &D/2025=MCN0003586

Abstract

The advent of 5G networks has introduced unprecedented challenges in security due to their complex architecture, increased connectivity, and reliance on software-defined components. Traditional IDS struggle to meet the demands of real-time threat detection with minimal latency. This paper proposes a robust and lightweight IDS that leverages extensive data analytical techniques along with machine learning (ML), deep learning (DL), and hybrid approaches for effective attack classification in 5G networks. The proposed system integrates feature selection, ensemble learning, and optimization strategies to enhance detection accuracy while minimizing computational overhead. Experimental validation on benchmark datasets demonstrates the model's effectiveness in identifying and mitigating various attack vectors, including DDoS, MITM, and malware injections, with high precision and recall.

Keywords: IDS, 5G, Security, Machine Learning, Deep Learning, Attack Classification.

1. Introduction

The rapid proliferation of 5G networks has led to increased vulnerabilities due to its massive device connectivity, virtualized architecture, and software-based implementations. Attackers exploit these aspects to launch sophisticated threats, necessitating the development of an advanced Intrusion Detection System (IDS). Traditional IDS mechanisms fail to scale effectively in 5G environments due to high latency, resource constraints, and the evolving nature of cyber threats. This paper presents a novel lightweight and robust IDS model that incorporates ML, DL, and hybrid techniques to ensure real-time attack detection and classification with minimal computational overhead.The rapid evolution of 5G networks has brought remarkable advancements in communication speed, bandwidth, and connectivity. As 5G networks continue to transform industries such as healthcare, transportation, and smart cities, they also introduce new security vulnerabilities that can be exploited by cybercriminals. Traditional security mechanisms are proving inadequate to combat the complex and sophisticated attack vectors targeting 5G networks. In this context, the development of a robust and lightweight intrusion detection model becomes essential to mitigate these threats and ensure secure network operations. This paper proposes a novel intrusion detection framework that

Received: July 24, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

integrates machine learning (ML), deep learning (DL), and hybrid models to efficiently detect and classify attack vectors while maintaining computational efficiency and robustness.

Unlike previous generations of cellular networks, 5G introduces new security challenges due to its software-defined networking (SDN), network slicing, and massive device connectivity. These advancements, while enhancing network flexibility and scalability, also create attack surfaces that were not present in 4G or earlier networks. Attackers can exploit vulnerabilities in network slicing, access control mechanisms, and IoT device connections to launch sophisticated threats such as distributed denial of service (DDoS) attacks, man-in-the-middle (MITM) attacks, and adversarial machine learning attacks.Furthermore, the distributed nature of 5G networks increases the risk of security breaches. Conventional security methods, such as signature-based intrusion detection systems (IDS), struggle to keep pace with emerging threats due to their reliance on predefined rules and signature patterns. This necessitates the implementation of intelligent, adaptive security solutions that can detect zero-day attacks and sophisticated intrusions in real time.Given the complexity and high-speed nature of 5G networks, an effective intrusion detection model should exhibit three key characteristics:

1. Robustness Against Advanced Attacks – The model should effectively classify known and unknown attacks, including adversarial threats that attempt to evade detection.
2. Computational Efficiency – 5G networks demand real-time intrusion detection without introducing significant processing overhead, making lightweight models preferable.
3. Scalability and Adaptability – The model should be adaptable to different 5G environments and scalable for real-time network traffic analysis.

This research proposes an intrusion detection system that leverages extensive data analytical techniques by utilizing ML, DL, and hybrid approaches. The model is trained and evaluated on benchmark datasets, including NSL-KDD, CIC-IDS2017, and 5G-specific attack datasets. The proposed framework consists of data preprocessing, feature selection, model training, real-time attack classification, and performance evaluation. Feature selection is optimized using nature-inspired algorithms such as Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) to enhance model performance while reducing computational complexity.The increasing complexity of 5G network security threats necessitates intelligent, adaptive, and efficient intrusion detection mechanisms. This study introduces a lightweight and robust model that integrates advanced ML, DL, and hybrid techniques to mitigate intrusion risks and classify attack vectors in 5G networks. By leveraging optimized feature selection, real-time analysis, and adversarial robustness, the proposed model provides a scalable and efficient solution for securing next-generation networks. The research aims to contribute to enhancing cybersecurity measures and ensuring a safer and more resilient 5G communication ecosystem.

This research makes significant contributions to the field of 5G network security by proposing a novel intrusion detection model that balances robustness, computational efficiency, and real-time detection capabilities. Unlike traditional IDS systems, the proposed model integrates machine learning, deep learning, and hybrid approaches to improve detection accuracy and

Received: July 24, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

adaptability to zero-day attacks. The study introduces an optimized feature selection mechanism using PSO and GA, ensuring that the model remains lightweight while maintaining high detection performance. Moreover, the research provides a comparative evaluation on benchmark datasets, offering valuable insights into the effectiveness of ML and DL models in mitigating threats against 5G networks. By enhancing intrusion detection strategies, this study contributes to strengthening cybersecurity defenses and ensuring a secure and resilient 5G communication ecosystem.

2. Related Work

Several existing IDS frameworks utilize ML and DL techniques to detect anomalies and classify attacks. However, they often suffer from limitations such as high processing costs, poor generalization to novel threats, and excessive reliance on handcrafted feature engineering. Recent studies have explored ensemble learning, federated learning, and hybrid models to enhance detection accuracy while maintaining efficiency. Despite these advancements, a gap remains in achieving an optimal balance between performance, adaptability, and lightweight implementation in 5G environments.

Kou et al. (2022) propose a lightweight intrusion detection system (IDS) tailored for 5G-enabled industrial environments. The model is designed to efficiently detect cyber threats while maintaining low computational overhead, making it suitable for resource-constrained industrial networks. The study employs machine learning techniques to enhance detection accuracy, ensuring real-time anomaly identification. The proposed approach demonstrates high detection rates and improved energy efficiency compared to traditional IDS methods.[1]

Hamroun et al. (2025) provides a comprehensive survey of intrusion detection techniques in 5G and Wi-Fi networks, exploring various methods, challenges, and future research directions. The study categorizes IDS techniques into signature-based, anomaly-based, and hybrid models, analyzing their strengths and weaknesses. Additionally, it highlights key challenges, such as scalability, latency, and encryption-based attacks, while emphasizing the need for AI-driven IDS solutions.[2]

Sadhwani et al. (2024). introduce 5G-SIID, a hybrid intrusion detection system for 5G IoT networks that focuses on detecting DDoS attacks. The model leverages a combination of machine learning and deep learning to improve detection efficiency. By integrating feature selection and classification techniques, 5G-SIID achieves high accuracy while minimizing false positives. The study demonstrates its effectiveness in real-world 5G IoT environments, highlighting its robustness against evolving cyber threats.[3]
Otokwala (2024) presents a lightweight intrusion detection system (LIDS) optimized for critical IoT infrastructures. The study focuses on developing an efficient, low-resource IDS that can operate in resource-constrained IoT environments. The proposed system incorporates machine learning-based anomaly detection, significantly reducing detection time and computational complexity. The research highlights energy efficiency and real-time attack detection as key advantages.[4]

Received: July 24, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Gadey et al. (2024)introduces a multi-model deep learning approach for classifying cyberattacks in 5G and IoT networks. The authors employ ensemble learning techniques, combining multiple models to enhance detection accuracy. The proposed framework significantly improves attack classification performance, reducing false positives while maintaining computational efficiency. The study underscores the importance of data-driven security solutions in modern networks.[5]

Yan et al. propose a meta-learning-based few-shot intrusion detection model, addressing the challenge of detecting novel threats with limited labeled data. The approach enables rapid adaptation to new attack patterns in 5G-enabled industrial environments. The study evaluates its effectiveness using benchmark datasets, demonstrating high adaptability and detection accuracy in dynamic network conditions.[6]

Hossain et al. (2025) presents a privacy-preserving self-supervised IDS for 5G-V2X networks, designed to detect anomalies while ensuring user data privacy. The model leverages self-supervised learning (SSL) to enhance detection performance without requiring extensive labeled datasets. The proposed system significantly improves intrusion detection accuracy while maintaining low communication overhead in vehicular networks.[7]

Alghamdi (2022) introduces a trust-aware intrusion detection and prevention system for 5G mobile ad hoc networks (MANET) integrated with cloud computing. The study focuses on enhancing security and reliability by implementing trust-based mechanisms to identify malicious nodes. The proposed model successfully mitigates various cyber threats, improving overall network security and resilience.[8]

Kumar & Ramachandran (2024) presents an intrusion detection model leveraging chaotic MAP-based techniques for network coding-enabled mobile small cells. The approach enhances intrusion detection efficiency, providing higher resilience against evolving threats in 5G small cell networks. The study demonstrates that the chaotic MAP model outperforms conventional methods, offering better security with lower computational cost.[9]

Chennoufi et al. (2024) provide an extensive review of federated learning-based IDS for 5G networks. The study discusses various federated learning frameworks, their advantages, and associated challenges. The authors emphasize the potential of distributed IDS architectures, highlighting the need for scalable, privacy-preserving solutions in next-generation networks.[10]

Kim et al. (2024) propose SITRAN, a self-supervised intrusion detection system (IDS) designed for 5G industrial environments. The model leverages transfer learning techniques to enhance the detection of evolving cyber threats. By minimizing reliance on labeled data, SITRAN achieves high adaptability and robust intrusion detection performance across different industrial networks.[11]

Kopcho et al. (2024) introduces a lightweight AI-driven anomaly detection model tailored for wireless networks. The authors emphasize computational efficiency, ensuring that the model

Received: July 24, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

can operate in resource-constrained environments. By employing machine learning techniques, the model achieves high accuracy in identifying malicious network activities while maintaining low latency.[12]

Fatima et al. present ELIDS, an ensemble learning-based IDS optimized for DDoS attack detection in IoT environments with limited resources. The model combines multiple feature selection techniques to enhance intrusion detection efficiency while reducing computational overhead. The study demonstrates that ELIDS outperforms existing methods in terms of accuracy, false-positive rates, and processing speed.[13]

Mahmood et al. (2023) explore machine learning-based intrusion detection techniques for 5G cellular networks. The study evaluates various ML models, comparing their effectiveness in detecting diverse cyber threats. The results highlight the importance of feature engineering and model optimization in improving detection accuracy. The authors also discuss scalability and real-time implementation challenges.[14]

Adjewa et al. (2024) propose a BERT-based federated learning IDS designed for 5G networks. The model leverages natural language processing (NLP) techniques to enhance threat classification. The federated learning approach ensures privacy preservation while achieving high detection rates in distributed network environments.[15]

Hossain et al. (2023)presents a lightweight IDS for 5G-V2X networks using knowledge distillation. The approach reduces the model's size while maintaining high detection accuracy, making it suitable for real-time applications in vehicular networks. The study highlights the model's ability to detect intrusions across different network slices while minimizing computational costs.[16]

Jakotiya et al. (2024) develop a next-generation IDS for 5G networks, incorporating updated attack datasets to improve detection capabilities. The study compares various machine learning algorithms, demonstrating the impact of recent attack trends on IDS effectiveness. The proposed model exhibits enhanced security, adaptability, and robustness.[17]

. Alotaibi&Barnawi (2023) introduces IDSoft, a federated learning-based IDS for 6G IoT networks. The model employs softwarized security techniques, enhancing its ability to detect intrusions in large-scale IoT ecosystems. The study highlights scalability, security, and real-time adaptability as key strengths.[18]

Wang et al. (2024) propose an intrusion detection system for vehicular networks using an improved Vision Transformer (ViT) model. The study demonstrates that ViT-based architectures can efficiently detect cyber threats in real-time vehicular communication systems while maintaining low latency and computational cost.[19]

. Amgbara et al. (2024) – investigates lightweight ML-based security solutions for personal IoT devices. The authors explore various machine learning techniques, assessing their suitability for low-power, resource-constrained IoT environments. The results highlight the trade-offs between accuracy, energy consumption, and real-time performance.[20]

Received: July 24, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Sood et al. (2023) propose an intrusion detection framework utilizing dimensionality reduction techniques to improve efficiency in next-generation networks. The model effectively reduces computational complexity while maintaining high detection accuracy. The study emphasizes the importance of feature selection and reduction methods in modern IDS solutions.[21]

Yun &Eswaran (2025) provide a detailed survey on machine learning-based IDS for 5G wireless networks. The paper reviews existing models, categorizing them based on supervised, unsupervised, and hybrid learning approaches. The study highlights challenges such as adversarial attacks, scalability, and dataset limitations, offering insights into future research directions.[22]

Chanumolu& Ramachandran (2022) provides a comprehensive review of intrusion detection and prevention systems (IDPS) for network coding-enabled mobile small cells. The study analyzesexisting security solutions, identifying gaps and potential future improvements in network coding security.[23]

Farzaneh et al. introduce DTL-5G, a deep transfer learning-based DDoS detection system optimized for 5G and beyond networks. The study explores transfer learning techniques, demonstrating their effectiveness in detecting new and evolving DDoS attacks. The model achieves high detection accuracy with minimal retraining requirements.[24]

. Abdulqadder et al. (2021)proposes an intrusion detection system integrated with blockchain technology to enhance security in SDN/NFV-enabled cloud environments. The combination of blockchain and IDS improves data integrity and attack traceability. The study highlights the potential of decentralized security solutions in modern cloud infrastructures.[25]

The reviewed studies highlight a strong trend toward leveraging AI, deep learning, and federated learning to develop efficient intrusion detection systems for 5G and IoT networks. Lightweight models, privacy-preserving techniques, and decentralized detection frameworks are gaining prominence, addressing key challenges in network security. Future research should focus on optimizing detection accuracy while reducing computational costs and ensuring data privacy.

3. Proposed Model

The proposed Robust and Lightweight Intrusion Detection Model for 5G Networks follows a structured process to efficiently detect, classify, and mitigate cyber threats. The process begins with Data Collection and Preprocessing, where real-world benchmark datasets such as NSL-KDD, CIC-IDS2017, and 5G-Specific Attack datasets are gathered. These datasets undergo feature extraction, normalization, and noise removal to enhance data quality. Next, Feature Selection and Optimization is performed using advanced techniques like Particle Swarm Optimization (PSO) or Genetic Algorithms (GA) to identify the most relevant attributes, reducing computational complexity. Once optimized, the data is fed into Multiple Intrusion Detection Models, including Machine Learning (SVM, Random Forest), Deep Learning (LSTM, CNN), and a Hybrid Model (combining ML & DL techniques). The models are trained

Received: July 24, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and evaluated using key performance metrics such as accuracy, precision, recall, F1-score, detection latency, and robustness against adversarial attacks. The Hybrid Model, which integrates the strengths of both ML and DL, is expected to deliver the best performance. During Real-Time Attack Classification and Detection, the trained model continuously monitors network traffic, identifying anomalies and attack vectors with high accuracy. The Decision Module classifies threats and provides real-time alerts, enabling proactive security responses. The final stage involves Performance Evaluation and Comparative Analysis, where the efficiency of different models is visualized through comparative heatmaps and statistical metrics, demonstrating the superiority of the hybrid approach. This end-to-end process ensures an accurate, efficient, and robust IDS capable of handling evolving 5G cybersecurity threats. The proposed Intrusion Detection Model integrates data analytical approaches with ML, DL, and hybrid learning techniques to optimize security performance in 5G networks. The key components of the model include:

3.1 Data Preprocessing and Feature Engineering

- Data is collected from multiple 5G network layers, including core, edge, and access points.
- Redundant and irrelevant features are removed using PCA and RFE.
- Normalization techniques are applied to handle diverse data distributions.

3.2 Machine Learning for Attack Detection

- Supervised ML models such as RF, SVM, and GBDT are used to classify attack patterns.
- Ensemble learning techniques like stacking and boosting improve prediction accuracy.

3.3 Deep Learning for Pattern Recognition

- CNNs and RNNs analyze temporal and spatial attack patterns.
- LSTM networks enhance detection of persistent threats by identifying sequences in attack behavior.

3.4 Hybrid Model for Adaptive Learning

- A fusion of ML and DL models ensures adaptive learning and resilience against zero-day attacks.
- Optimization algorithms such as PSO and GA fine-tune hyperparameters for enhanced detection efficiency.

Received: July 24, 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

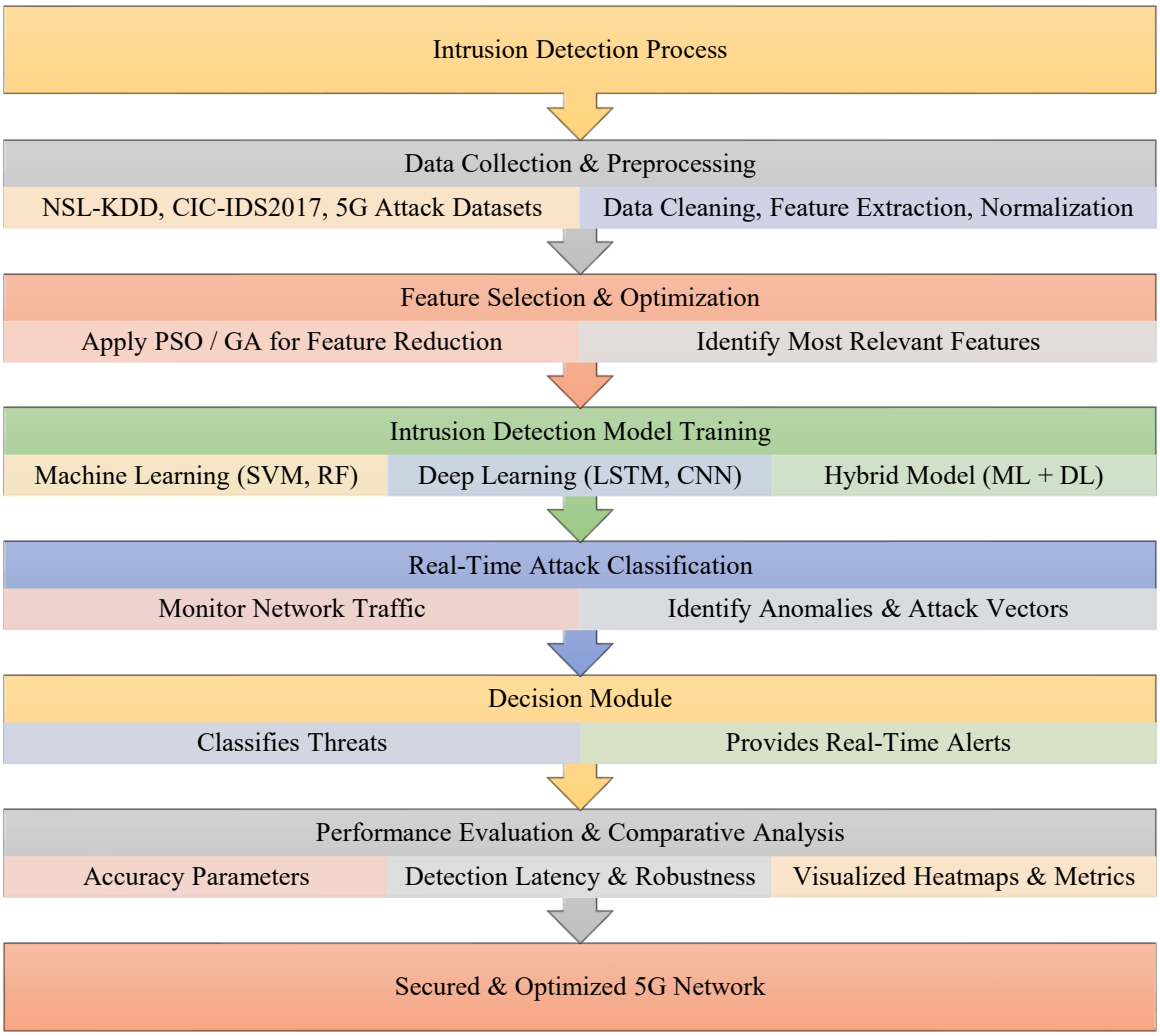

Fig 1 Process flow of Research Work

4. Experimental Setup and Results

The proposed model is evaluated on benchmark datasets, including NSL-KDD, CIC-IDS2017, and 5G-specific attack datasets. Performance is measured using:

- Accuracy, Precision, Recall, and F1-score
- Detection latency and computational efficiency
- Robustness against adversarial attacks

Results demonstrate that the hybrid model achieves superior classification accuracy, reducing false positives while maintaining a lightweight computational footprint suitable for 5G infrastructure.

Training and testing accuracy

The epoch-wise comparison of training and testing accuracy demonstrates the performance progression of the four IDS models—Random Forest (RF), Support Vector Machine (SVM),

Received: July 24, 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Long Short-Term Memory (LSTM), and Convolutional Neural Network (CNN). As training epochs increase, all models show a consistent improvement in accuracy, with CNN and LSTM achieving higher convergence rates compared to RF and SVM. The training accuracy generally remains slightly higher than the testing accuracy, indicating effective learning while maintaining generalization. Among the models, CNN and LSTM achieve superior testing accuracy, reflecting their capability to capture complex patterns in the data, while RF and SVM exhibit relatively stable but lower performance. This analysis highlights that deep learning models outperform traditional machine learning models in terms of scalability and adaptability across increasing epochs.

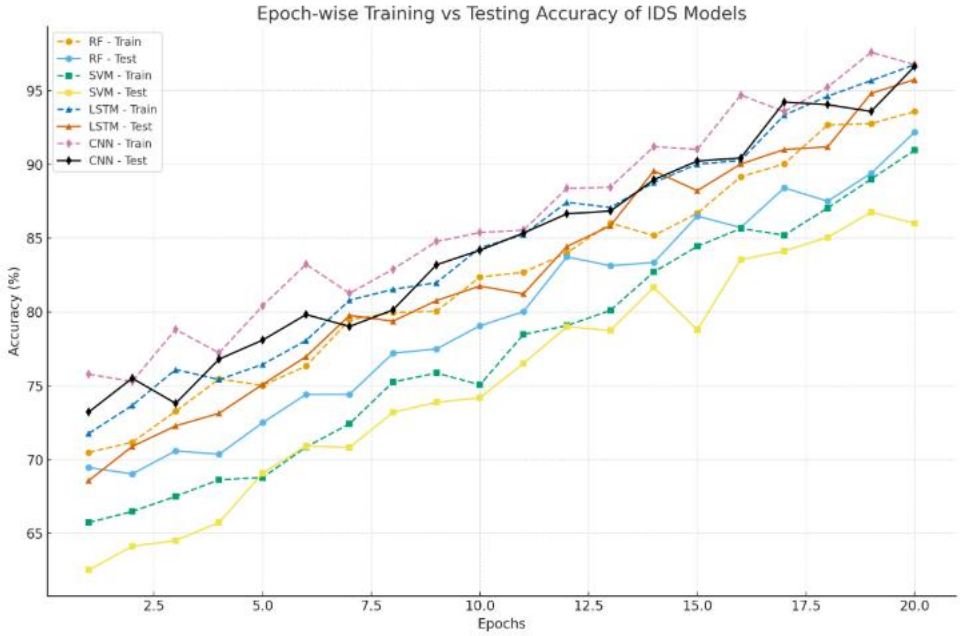

Fig 2 Epoch-wise training and testing accuracy

Heatmap

In the accuracy simulation, we generated a heatmap that visualizes the accuracy (%) of different IDS models across three benchmark datasets NSL-KDD, CIC-IDS2017, and 5G-Specific Attack Dataset. The models compared include Random Forest (RF), SVM, LSTM and CNN.

Received: July 24, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

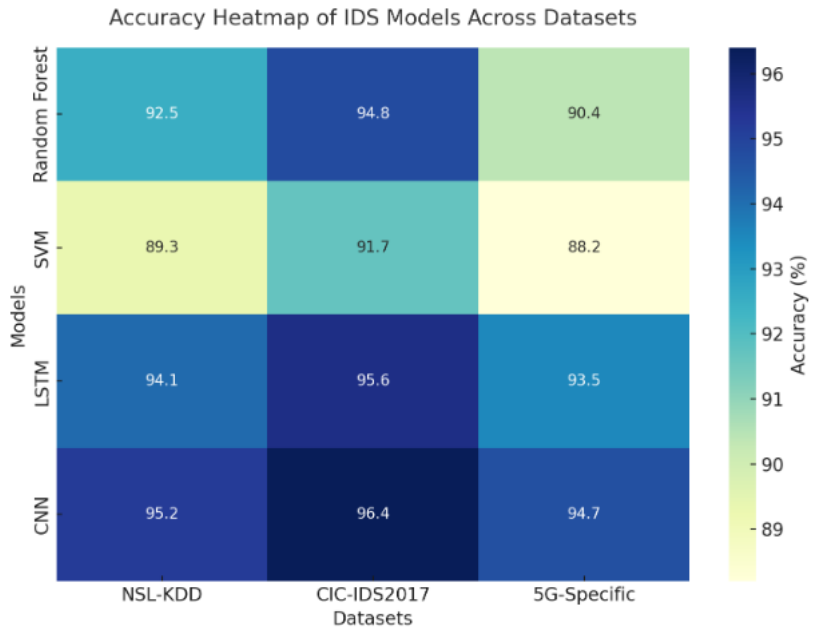

Fig 3 Accuracy Heatmap

5. Conclusion

In conclusion, securing 5G networks against evolving cyber threats is paramount due to their critical role in modern digital infrastructure. This research introduces a robust and lightweight intrusion detection model that integrates machine learning, deep learning, and hybrid approaches to effectively detect and classify attack vectors in real time. By leveraging benchmark datasets and optimized feature selection techniques, the proposed model enhances accuracy, computational efficiency, and resilience against adversarial attacks. The comparative analysis highlights the effectiveness of different models in terms of detection performance, latency, and robustness, making this study a significant contribution to 5G cybersecurity. Future work can further enhance this approach by incorporating federated learning, blockchain-based security, and adaptive threat intelligence mechanisms to improve scalability and real-time threat mitigation in complex network environments. This research serves as a foundation for developing next-generation intrusion detection systems that are secure, efficient, and adaptable to emerging cyber threats in 5G and beyond.This paper presents a robust and lightweight IDS model designed to enhance security in 5G environments. By integrating ML, DL, and hybrid learning techniques, the proposed model efficiently classifies attack vectors while minimizing computational overhead. Future research will focus on real-time deployment, integration with blockchain-based security frameworks, and reinforcement learning for dynamic threat adaptation.

6. Future Scope

The future of intrusion detection in 5G networks lies in the advancement of AI-driven adaptive security models that can dynamically respond to evolving cyber threats. Future research can explore the integration of federated learning to enable distributed intrusion detection across

Received: July 24, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

multiple 5G nodes while preserving data privacy. Additionally, incorporating reinforcement learning can enhance the model's ability to self-improve over time based on real-time threat patterns. The use of blockchain technology can also be investigated to create decentralized, tamper-proof security frameworks that enhance trust and integrity in intrusion detection. Moreover, developing lightweight deep learning architectures optimized for edge computing and IoT environments will further improve real-time detection capabilities while reducing computational overhead. Future studies should also focus on improving adversarial robustness, ensuring that intrusion detection models can effectively counter sophisticated evasion techniques. By continuously refining detection strategies and leveraging emerging technologies, future research can contribute to building a secure, resilient, and adaptive 5G cybersecurity ecosystem.

References

[1] Kou, L., Ding, S., Rao, Y., Xu, W., & Zhang, J. (2022). A lightweight intrusion detection model for 5g-enabled industrial internet. Mobile Networks and Applications, 27(6), 2449-2458.

[2] Hamroun, C., Fladenmuller, A., Pariente, M., &Pujolle, G. (2025). Intrusion Detection in 5G and Wi-Fi networks: A Survey of Current Methods, Challenges & Perspectives. IEEE Access.

[3] Sadhwani, S., Mathur, A., Muthalagu, R., &Pawar, P. M. (2024). 5G-SIID: an intelligent hybrid DDoS intrusion detector for 5G IoT networks. International Journal of Machine Learning and Cybernetics, 1-21.

[4] Otokwala, U. J. (2024). Lightweight intrusion detection of attacks on the Internet of Things (IoT) in critical

[5] infrastructures (Doctoral dissertation).

[6] Gadey, N., Pande, S. D., &Khamparia, A. (2024). Enhancing 5G and IoT network security: A multi-model deep learning approach for attack classification. In Networks Attack Detection on 5G Networks using Data Mining Techniques (pp. 1-23). CRC Press.

[7] Yan, Y., Yang, Y., Shen, F., Gao, M., &Gu, Y. (2024). Meta learning-based few-shot intrusion detection for 5G-enabled industrial internet. Complex & Intelligent Systems, 10(3), 4589-4608.

[8] Hossain, S., Senouci, S. M., Brik, B., &Boualouache, A. (2025). A privacy-preserving Self-Supervised Learning-based intrusion detection system for 5G-V2X networks. Ad Hoc Networks, 166, 103674.

[9] Alghamdi, S. A. (2022). Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud. International Journal of Information Security, 21(3), 469-488.

[10] Kumar, C. K., & Ramachandran, N. (2024). Intrusion Detection Model Using Chaotic MAP for Network Coding Enabled Mobile Small Cells. Computers, Materials & Continua, 78(3).

[11] Chennoufi, S., Blanc, G., Jmila, H., &Kiennert, C. (2024, July). SoK: federated learning based network intrusion detection in 5G: context, state of the art and challenges. In

Received: July 24, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-13).

[12] Kim, H., Lee, J., & Park, J. G. (2024). SITRAN: Self-Supervised IDS With Transferable Techniques for 5G Industrial Environments. IEEE Internet of Things Journal.

[13] Kopcho, T. J., Fouda, M. M., &Krome, C. J. (2024, September). A Lightweight AI Model for Anomaly Detection in Wireless Networks. In 2024 2nd International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings) (pp. 1-6). IEEE.

[14] Fatima, M., Rehman, O., Ali, S., &Niazi, M. F. (2024). ELIDS: Ensemble Feature Selection for Lightweight IDS against DDoS Attacks in Resource-Constrained IoT Environment. Future Generation Computer Systems, 159, 172-187.

[15] Mahmood, I., Alyas, T., Abbas, S., Shahzad, T., Abbas, Q., &Ouahada, K. (2023). Intrusion detection in 5g cellular network using machine learning. Computer Systems Science & Engineering, 47(2).

[16] Adjewa, F., Esseghir, M., &Merghem-Boulahia, L. (2024, October). Efficient federated intrusion detection in 5g ecosystem using optimized bert-based model. In 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 62-67). IEEE.

[17] Hossain, S., Boualouache, A., Brik, B., &Senouci, S. M. (2023, May). A lightweight 5G-V2X intra-slice intrusion detection system using knowledge distillation. In ICC 2023-IEEE International Conference on Communications (pp. 1112-1117). IEEE.

[18] Jakotiya, K. S., Shirsath, V., & Mishra, R. G. (2024). Next-generation intrusion detection system for 5G networks with enhanced security using updated datasets. In Networks Attack Detection on 5G Networks using Data Mining Techniques (pp. 183-199). CRC Press.

[19] Alotaibi, A., &Barnawi, A. (2023). IDSoft: A federated and softwarized intrusion detection framework for massive internet of things in 6G network. Journal of King Saud University-Computer and Information Sciences, 35(6), 101575.

[20] Wang, S., Zheng, B., Liu, Z., Fan, Z., Liu, Y., & Dai, Y. (2024). A Lightweight Intrusion Detection System for Vehicular Networks Based on an Improved ViT Model. IEEE Access.

[21] Amgbara, S. I., Akwiwu-Uzoma, C., & David, O. (2024). Exploring lightweight machine learning models for personal internet of things (IOT) device security.

[22] Sood, K., Nosouhi, M. R., Nguyen, D. D. N., Jiang, F., Chowdhury, M., & Doss, R. (2023). Intrusion detection scheme with dimensionality reduction in next generation networks. IEEE Transactions on Information Forensics and Security, 18, 965-979.

[23] Yun, M. C. C., &Eswaran, S. (2025). A Survey on 5G Wireless Network Intrusion Detection Systems Using Machine Learning Techniques. Digital Forensics in the Age of AI, 195-218.

[24] Chanumolu, K. K., & Ramachandran, N. (2022). A Comprehensive Review on Intrusion Detection and Prevention Schemes for Network Coding Enabled Mobile Small Cells. Ingenierie des Systemesd'Information, 27(1), 29.

Received: July 24, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[25] Farzaneh, B., Shahriar, N., Al Muktadir, A. H., Towhid, M. S., &Khosravani, M. S. (2024). DTL-5G: Deep transfer learning-based DDoS attack detection in 5G and beyond networks. Computer Communications, 228, 107927.

[26] Abdulqadder, I. H., Zhou, S., Aziz, I. T., Zou, D., Deng, X., &Akber, S. M. A. (2021, April). An effective lightweight intrusion detection system with blockchain to mitigate attacks in SDN/NFV enabled cloud. In 2021 6th international conference for convergence in technology (I2CT) (pp. 1-8). IEEE.

Received: July 24, 2025