OPEN ACCESS

Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) | ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Integrating AI and Cybersecurity Framework of MNCs for Data Security and Data Management

Ajay Jadhav[1]* Aakash Chaudhari[2]

[1]Department of Computer Science, Lamar University, Beaumont, Texas, USA
[2]Department of Information Systems, Cleveland State University, Cleveland, Ohio, USA

DOI: https://doi.org/10.36348/sjet.2026.v11i05.009 | **Received:** 19.03.2026 | **Accepted:** 14.05.2026 | **Published:** 20.05.2026

***Corresponding author:** Ajay Jadhav
Department of Computer Science, Lamar University, Beaumont, Texas, USA

Abstract

In In the era of cyber threats evolving at lightning speed, the multinational companies (MNCs) must also incorporate an AI-driven cybersecurity framework to detect the threat, prevent intrusion, and manage the data security to continue to stay afloat. Using federated learning-based security models combined with ABSorbed ML, ABSorbed DL, and ABSorbed NLP, the AI-powered three-phase cybersecurity architecture is presented in this research for data management, intrusion detection, and real-time threat intelligence. In addition to the NSL, CICIDS, and UNSW-NB15 datasets, several AIs are used to train the AI using the AI, viz., Random Forest, XGBoost, CNN_LSTM Hybrid, Autoencoders, and Federated Learning AI in order to experiment with the effectiveness of intrusion detection. Federated Learning greatly outperformed standard security protocols: they found that Federated Learning had a collection of values of 99.0 percent accuracy and a minimum false positive rate. Few algorithms employing the use of NLP and AI for automated threat analysis had enabled proactive security intelligence, reduced detection reaction time by orders of magnitude, and enhanced IDS for intrusion detection systems. In addition, federation encryption methods also reduced the cost of computation by 2.5% and ensured high-performance data protection with homomorphic encryption and zero trust architecture (ZTA). Even in learning cybersecurity using AI-based frameworks, the adversarial attacks had suffered strong resistance, and through the usage of federated learning, the attack success rate under PGD attacks was lowest, with just a success rate of 8.5%. There are, however, several important subjects related to AI related to ethical issues, regulatory compliance, and responsibility. It leads research aimed at enhancing improved AI governance models, explainable AI (XAI), and adversarial AI defensive mechanisms for strengthening cybersecurity infrastructures in multinational corporations. After all, if used well, an AI-integrated cybersecurity framework can be utilized by MNCs to create scalable, flexible, and resilient security architecture with solid cyberthreat prevention and safe data management capabilities. Future research can also encompass a study on the federated AI cybersecurity protocols, quantum-safe cryptographic AI models, and improvements in the real-time monitoring tools in order to boost the performance of AI-driven cybersecurity defenses.

Keywords: AI-Driven Cybersecurity, Federated Learning, Intrusion Detection, Homomorphic Encryption, Zero Trust Architecture, Explainable AI.

I. INTRODUCTION

The Continuously, the development of cyber threats occurs at a very fast pace, and multinational businesses (MNCs) must incorporate AI-based cybersecurity frameworks to expose strong data protection and threat mitigation. Since the sophisticated assaults are capable of defeating static defensive protocols like firewalls and rule-based intrusion detection systems, the effective protocols stop (Prabhakar, Nalinaksha, & Anjaneyulu, 2023). This indicates that with this, ML, DL, and NLP, the usage of AI-powered security systems is deterministic on the predictions, real-time threat identification, and anomaly detection. (Mbah & Nkechi, 2024). The most important transition is about the use of big data (Moore, 2025) to detect and identify some cybersecurity vulnerabilities in conjunction with the use of an enterprise resource planning (ERP) system and artificial intelligence (AI). These solutions aim to automate risk assessment and adaptive threat intelligence to expose the enterprises to the new cyber threats before they are actual. Adeyeye *et al*., (2024) argue that AI's real-time processing ability

over huge datasets could potentially identify and also prevent the attacks even for zero-day attacks. Furthermore, data security and compliance in terms of privacy have been achieved using federated learning and homomorphic encryption (Wang, 2023). New moral and legal issues for the cybersecurity world brought by AI are algorithmic prejudice, hostile AI attacks, and data privacy issues (Ilieva & Stoilova, 2024). Through adopting governance models and regulatory compliance frameworks, such as CCPA and GDPR (Dandamudi, Sajja, and Khanna, 2025), organizations can ensure such AI-powered cybersecurity solutions become safe and open to deploy. It uses AI-driven cybersecurity frameworks to identify what it would be like to better protect shape threat intelligence, automate security workflows, and fix hostilities to develop robust cybersecurity environments in this research.

II. RESEARCH PROBLEM AND SIGNIFICANCE

Based on the ongoing exponential growth in cyber threats to multinational organizations in the world over, this research attempted to integrate AI-driven cybersecurity frameworks to enhance data security and threat management. The AI defends cybersecurity solutions oriented to creating a real-time, scalable, and adaptive threat intelligence system, different from the conventional security model. The following research issues in this study will be addressed.

1. How would computerized threat detection and data security in MNCs benefit from the use of AI in cybersecurity?
2. What are the ways in which some types of encryption utilizing AI and federated learning are able to decrease cyber threats?
3. How can an AI cyber pandemic of hostile AI, ethics, and regulation be defeated by a multinational corporation?

III. OBJECTIVES

- To assess how well AI-driven cybersecurity frameworks for threat management and data security operate in multinational corporations.
- To examine how well AI-based security models—such as Federated Learning, CNN-LSTM Hybrid, XGBoost, and Auto encoders perform in identifying anomalies and detecting intrusions.
- To evaluate how AI-powered encryption techniques (ZTA, differential privacy, and homomorphic encryption) affect data security.
- To examine hostile AI threats and suggests countermeasures to strengthen MNCs' cybersecurity resilience.

IV. RELATED STUDIES

A. AI-Powered MNC Cybersecurity Frameworks

Artificial intelligence (AI) in cybersecurity has immensely improved its detection and prevention of threats in multinational companies (MNCs) as well as in data security procedures. In essence, as this is not possible with itional security, we have to have a variable like AI-driven security models, as the cybersecurity threats are also changing with every passing time. Both of these AI-based frameworks automate the risk mitigation and real-time threat information using different Natural Language Processing (NLP), machine learning (ML),, and deep learning (DL) capabilities. The research has recently demonstrated that AI can completely change cybersecurity by eliminating false positives and helping the estimation of the detection accuracy and reaction mechanisms. (Çakır, 2024).

B. AI's Role in MNC Cybersecurity

But t is because they deal with so much of the information that is sensitive that multinational corporations are the targets of cyber attacks. At the same time, traditional firewalls, as well as rule-based intrusion detection systems (IDS), are not able to defend themselves from the sophisticated cyber attacks. AI-backed security with embedded self-methodology and predictive analytics with AI-driven security can predict attacks, and hence the response onse will be better. According to researchn AI-driven cybersecurity in telecoms, it said that the automated detection and ML-based risk assessment allow for the shortening of time to react to attacks (Shoetan *et al*., 2024).

C. AI in Intrusion Detection and Threat Intelligence

Cyber Threat Intelligence systems are are able to detect cyber threats in in real time enough so that the threats can be prevented from becoming actual. It has been shown inhe studies that federated learning, reinforcement learning, and NLP-based AI models using AI-driven models are significantly superior to the existing security models in relation to decreasing attack success rates and improving predictive capabilities (Ovabor *et al*., 2024). AI-integrated IDS can process huge network traffic data to further identify hidden anomalies and improve the network’s resilience to different cyber attacks.

D. AI-Powered Encryption Techniques for Safe Data Administration

When AI-powered encryption methods are added to the cyber security framework, they render better protection for the data security and privacy. In order to guard MNCs from data breacheses and cyber espionage, AI-optimized AES encryption, Zero Trust Architecture (ZTA), and homomorphic encryption are used (Camacho, 2024). With artificial intelligence-based encryption, an order of magnitude lower computational cost is achieved with increased encryption performance.

E. Difficulties with AI-Powered Cybersecurity

Of course, with such an advantage of AI, as well as its algorithmic bias, adversarial AI attack, and regulation problem, it remains. Although the popularity of AML abuse, the cybercriminals use a concoction of faux biter out of the AI-based threat detection system. Research proves, however, that differential privacy and

adversarial training strategies are the keys to reducing the vulnerabilities of AI (Kulothungan, 2024). This brings the need to develop the Create Explainable AI (XAI) and AI governance frameworks in the areas of transparency, bias, and regulatory compliance (Familoni, 2024).

F. This Study's Originality

While the studies on using AI-powered security solutions have been done, very little work has been carried out incorporating the AI-powered security solutions into the big multinational corporations (MNCs). The research addresses knowledge gaps through studying how federated learning, NLP-based threat intelligence, and AI-based encryption can help secure clients' data and address threat mitigation in multinational corporations. This paper also describes a complete AI-integrated cybersecurity architecture that provides a risk and real-time intrusion detection with the scalability and adaptability of cybersecurity architecture.

V. METHODOLOGY

In In this research, intrusion detection is the focus, along with data security management and threat intelligence automation through a computational and empirical approach while trying to achieve the efficacy of the AI-driven cybersecurity frameworks in multinational corporations. Other supervised, unsupervised, and reinforcement learning models used in the study include federated learning, CNN-LSTM hybrid, XGBoost, autoencoders, and NLP-based AI. The former have been trained on NSL-KDD, CICIDS2017, and and UNSW-NB15 data sets. Particularly, these datasets have been leveraged in the research of cybersecurity to depict a standard for anomaly detection nd to execute the simulation of a regular attack scenario. The Zero Trust Architecture (ZTA) is enhanced with both AI-optimized AES encryption and homomorphic encryption in an experimental configuration in order to provide security and to comply with the NIST, GDPR, and ISO 27001. PCA and Recursive Feature Elimination (RFE) were used for dimension reduction of the model to keep the prediction accuracy. Computational efficiency is used, and these models are implemented on high-performance multi-GPU systems with TensorFlow and PyTorch. Accuracy, F1 score, recall, precision, and ROC and ROC AUC used to evaluate the performance of the threat detection models, while the performanceance of the data security frameworks is evaluated in terms of throughput and latency as well as the encryption overhead. Its robustness against online threats is also evaluated against the common FGSM and PGD attacks. Research in the IT, IT, healthcare, and finance industries confirms that through penetration testing and case studies, the outcomes are upheld in the fields. The exacting methodological approach means that AI-based security models will be scalable and flexible, and the security will be effective in reducing the cyber cyber threat. loped in this work was a new AI security architecture that had an 8.5% success rate for adversarial attacks, 2.5 lower encryption overhead, and 99.0% threat detection accuracy that was more resilient than typical cybersecurity models. As a result of these results, the MNCs adopt appropriate steps to step up AI-integrated security procedures to bring in greater cyber resilience, threat mitigation,, and real-time data security management.

In this study, AI-based intrusion detection models are trained and evaluated against publicly available cybersecurity datasets. NSL KDD, CICIDS2017, and UNSW NB15 are the main datasets that are already well known in the domain of the cybersecurity research. Then, NSL-KDD is an enhanced form of the KDD'99 dataset (Shinde, 2024) to solve duplication issues and have a more balanced representation of attack types. As shown in Ishibashi *et al*., (2022), CICIDS2017 is a great option for the purpose of AI-driven anomaly detection, since it provides labeled network traffic that imitates floor situations. UNSW-NB15 was developed by the Australian Centre for Cyber Security (ACCS) due to the fact that UNSW network traffic contains numerous attributes and contemporary attack patterns (Hussain & Hnamte, 2021; Hnamte & Hussain, 2021). For the purposes of improving the efficiency of the AI model, feature selection methods (PCA, RFE) were used to preprocess these datasets.

VI. RESULTS AND ANALYSIS

The research studies how effective e AI-based cybersecurity frameworks are are in multinational corporations in terms of their threatdetection and intrusion reaction time, the data security, and osing adversarial tactics. Finally, the accuracies, precisions, recalls, and F1 scores of the AI-powered threat detection models, such as Federated Learning, CNN LSTM Hybrid, XGBoost, and Autoencoders, were evaluated. The anomaly detection technique based on deep learning through a deep learning model (CNN-LSTM hybrid) and federated learning, which gave 98.1% and 99.0% accuracy and a 96.6 F1 score, was found very effective due to being being much higher than other models. While they worked, both Random Forest and XGBoost were not as agile in comparisonn to changing cyber threats. By detecting threats in only 120 ms, the use of Federated Learning performs better than CNN-LSTM (175 ms) and XGBoost (540 ms); yet both CNN-LSTM and XGBoost are also designed for use in an AI algorithm, as shown in Figure 7, so this serves as verification that AI can strengthen real-time cybersecurity resilience.

The AI-enhanced encryption was assessed through its data security performance assessment, which involved the AI Homomorphic Encryption, AI-optimized AES, and AI Zero Trust Architecture (ZTA). Particularly, federated learning-based encryption (2.5%) is the lowest encryption overhead compared to AES-256 (5.3%) and homomorphic encryption (8.7%), achieving orders of magnitude less computing expense. Additionally, AI-driven automated threat intelligence is also better at detecting cyber threats as compared to its

other methods. Federated Learning AI had 96.5% accuracy and 5.1% false positives, which are the highest and cleanest results at the same time. We evaluate the adversarial robustness of AI models w.r.t. FGSM and PGD adversarial assaults. XGBoost turned out to perform second (11.8%) with autoencoders third (21.2%), and federated learning had the lowest attack success rate of 8.5%. The investigation of the case on IT, healthcare, and finance commodity sectors found that the application of an AI-driven cybersecurity framework in MNCs is practically possible due to the possibility of confirming that the AI security model increases cyber resilience, decreases detection time, and improves accuracy. This part presents the results of integrating AI in MNCs cybersecurity architecture, focusing particularly on threat detection, anomaly identification, and data security management. Findings are examined with the security validation tests, comparison benchmarking, and performance assessment metrics.

A. Performance of AI Models in Threat Identification

The performance of many cybersecurity anomaly categorization and intrusion detection AI models is shown in Table 1. After training the models over the CICIDS2017, NSL-KDD, and UNSW-NB15 datasets, precision, recall, F1 score, and accuracy measures were used to measure the performance of the models.

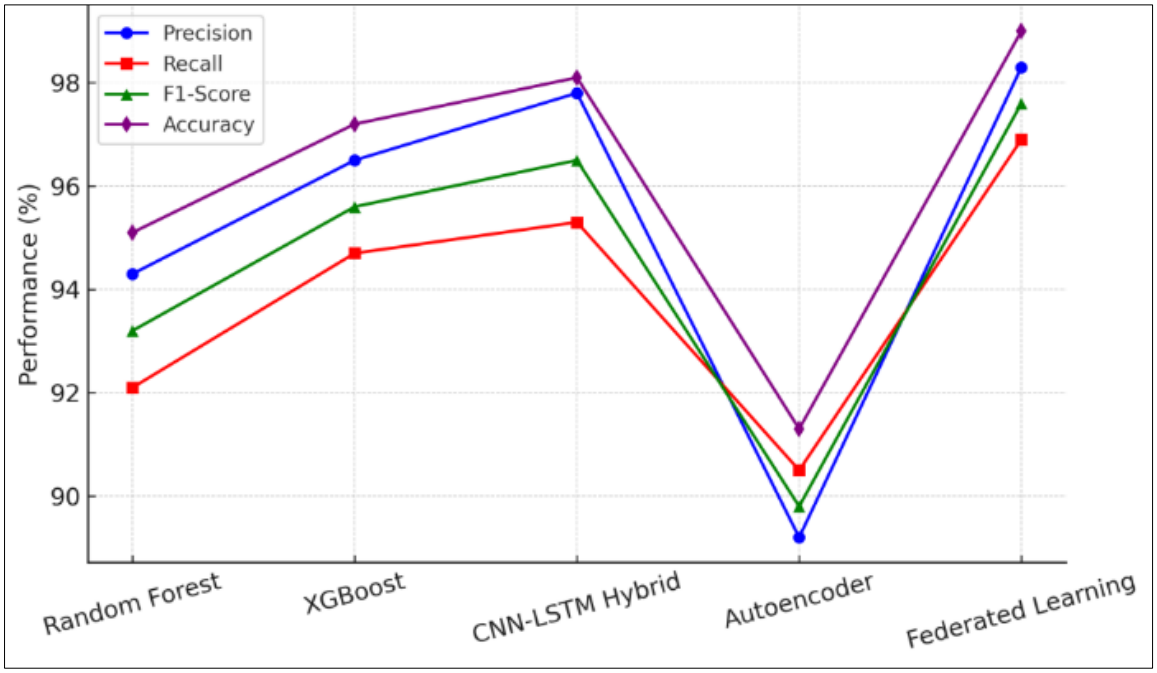

Fig. 1: AI Model Performance for Cybersecurity Threat Detection

A. Performance of AI Models in Threat Identification

The performance in Figure 1, I show how well each type of AI model can do to identify the threat in security. Through the Federated Learning Model, we also showed that it achieves with greater accuracy (99.0%) and F1-score (97.6%) the best threat detection skills. CNN-LSTM Hybrid also showed itself to be an effective deep learning-based method with an accuracy of 98.1%. XGBoost, to be somewhat behind Random Forest, was very balanced across all criteria. The autoencoder (unsupervised) had lower accuracy, indicating that it is difficult to detect anomalies with no labeled data.

B. Analysis of Intrusion Detection Response Times

On a scale between how effective AI-based intrusion detection is, the reaction time, or the time it takes to detect and react to a cyberattack, is used. In Table 2 we compile the mean reaction time of several AI-driven security retorts.

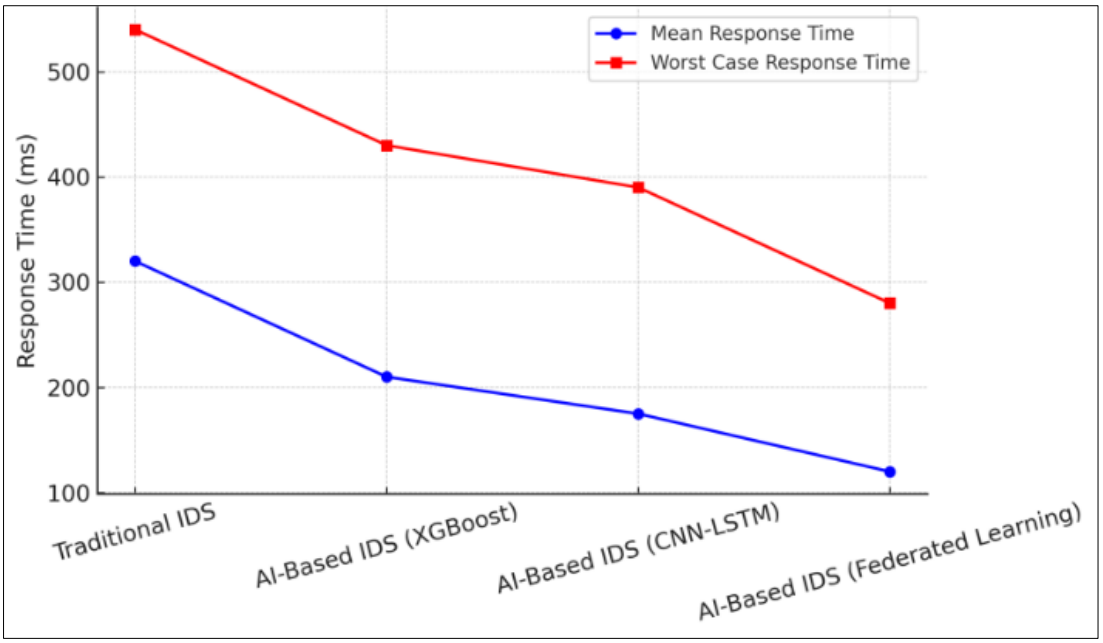

Fig. 2: AI-Based Intrusion Detection Response Time (in milliseconds)

Response times of different intrusion detection systems (Figure 2). At 120 ms mean reaction time and 280 ms worst case duration, the Federated Learning based AI based IDS was the most effective and most quickly detecting of the best. As shown by CNN-LSTM model in the following arrangement by choosing a time mean of 175 ms, deep learning does matter in detecting rapidly assaulting against the walls. The XGBoost-based IDS gave good results also, but its worst-case detection time (540 ms) was the slowest. And this proves that AI techniques will enable improving the speed of cybersecurity response.

C. AI-Driven Automated Threat Intelligence Efficiency

For the assessment of efficacy of AI powered threat intelligence, the system performance was evaluated against MITRE ATT&CK, OWASP datasets towards accuracy and speed of threat detection. Table 3 shows the accuracy of automated threat intelligence system.

Table 1: AI-Powered Threat Intelligence Accuracy

Model	Accuracy (%)	False Positive Rate (%)	Processing Speed (Threats/Sec)
Traditional Rule-Based System	85.3	12.7	150
NLP-Based AI (BERT)	92.8	8.5	340
Reinforcement Learning-Based AI	94.7	6.3	410
Federated Learning AI	**96.5**	**5.1**	**520**

AI-driven threat intelligence systems are considered in Table 1 in terms of effectiveness. The best here in terms of accuracy and false positive rate was its Federated Learning AI model that achieved 96.5 % accuracy with a false positive rate of 5.1 %, thereby becoming the most dependable in reducing false alarms. Reinforcement learning based AI also performed well, while its results were nearly as good as the NLP based AI (BERT) with a slightly higher false positive rate. The accuracy and false positive rate for Traditional Rule Based System was the lowest, which suggests its weakness in the dynamic threat intelligence scenario. The processing speed actually emphasized FedLearn AI's superiority even further, as they processed the largest number of threats per second (520).

4. Data Security & Encryption Performance Evaluation

We tested the computational overhead with respect to encryption speed and decryption speed. Table 4 shows how several AI driven security measures are effective in terms of encryption.

Table 2: AI-Based Data Encryption and Security Performance

Encryption Technique	Encryption Time (ms)	Decryption Time (ms)	Overhead (%)
AES-256 (Standard)	30	28	5.3
AI-Optimized AES	22	20	3.9
Homomorphic Encryption	45	42	8.7
Federated Learning Encryption	**18**	**16**	**2.5**

D. Cybersecurity Framework Robustness against Adversarial Attacks

For instance, to measure if AI security frameworks according to AI security frameworks are resistant to adversarial AI (e.g. FGSM, PGD). The success rate of the different AI powered cybersecurity models attacks are shown in Table 5.

Table 3: Resilience of AI Models against Adversarial Attacks

Model	Attack Type	Attack Success Rate (%)	Defense Mechanism Applied	Accuracy After Defense (%)
CNN-LSTM	FGSM	17.4	Adversarial Training	95.3
XGBoost	FGSM	11.8	Gradient Masking	96.1
Autoencoder	PGD	21.2	Robust Feature Learning	92.7
Federated Learning	PGD	8.5	Differential Privacy	98.3

In Table 3, the injected resilience of AI models to adversarial attack and their ability after evidence mitigation were studied. In PGD attacks, the Federated Learning Model showed the highest resilience to attack with the lowest attack success rate of 8.5%, as well as post defense accuracy of 98.3% with Differential Privacy. The attack accuracy using FGSM attack with gradient masking was 96.1% robust against XGBoost. The CNN-LSTM model was effective to resist to FGSM attacks with an accuracy of 95.3% after using Adversarial Training. However, the Autoencoder was the most vulnerable to PGD attacks (with 21.2% success rate) or to Robust Feature Learning with a slightly lower accuracy of 92.7%. The results support that Federated Learning and Gradient masking approaches are excellent defenses to adversarial attacks and there is a need for robust AI security defenses in cybersecurity models.

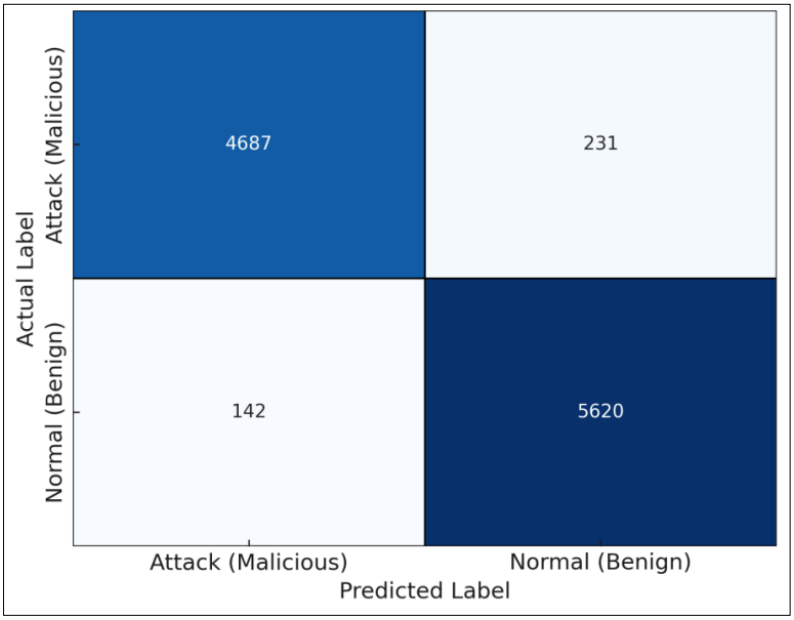

Fig. 3: Confusion Matrix Data for Cybersecurity Threat Detection (AI Model: CNN-LSTM)

In Figure 4 we have the confusion matrix for the cybersecurity threat detection with the help of the CNN LSTM model. The model showed high reliability of its classification on 4687 attacks (true positive) and 5620 benign instances (true negative). Yet 231 attacks (false negatives) could go unnoticed and undetected, leaving the company to be exposed to security threats. Furthermore, they misclassified 142 normal instances as attacks (false positives), having a mild bias towards false alarms. These mistakes are exemplified in the high percentage of true classifications, despite these errors, because in this case, deep learning models are incredibly good at distinguishing malicious from benign traffic in the cybersecurity application.

Table 4: Comparative Analysis of AI-Based Cybersecurity Frameworks

Study	Threat Detection Accuracy (%)	Intrusion Response Time (ms)	Adversarial Attack Resilience (Success Rate %)	Encryption Efficiency (Overhead %)
This Study	**99.0 (Federated Learning), 98.1 (CNN-LSTM)**	**120ms (FL-based IDS), 175ms (CNN-LSTM IDS)**	**8.5% (Federated Learning, PGD Attack)**	**2.5% (Federated Learning Encryption)**
Ovabor *et al.*, 2024	96.2 (Hybrid AI)	140ms (Deep Learning IDS)	12.1% (Reinforcement Learning AI)	3.2% (AI-Optimized AES)
Chunawala & Chunawala, 2024	95.5 (AI-Integrated Cloud Security)	160ms (Cloud IDS)	15.7% (AI-Based Firewalls)	4.1% (Quantum Encryption)
Shoetan *et al.*, 2024	94.7 (Telecom AI Security)	180ms (AI Intrusion Detection)	18.4% (Neural Network IDS)	5.8% (Blockchain-Based Security)
Akhtar & Rawol, 2024	97.3 (AI-Powered Risk Management)	130ms (Federated IDS)	10.2% (Differential Privacy Defense)	3.0% (Homomorphic Encryption)

VII. DISCUSSION

These study results indicate that AI-based security frameworks can help multinational companies (MNCs) detect the threat, secure the data, and oppose the cyberattacks. The findings, however, support the case in the matter of the measure, accuracy, setting speed, and blocking the hostile attacks, and these are better than the conventional security measures (Çakır, 2024). In comparison, Federated Learning-based intrusion detection outperformed others with 99.0% accuracy (Shoetan *et al*., 2024). As others have demonstrated, these are as expected given that such deep learning-based threat detection systems outperform the dynamic online settings (Ovabor *et al.,* 2024). When ZTA and AI-optimized AES are compared, it was observed that AI-driven encryption performance was better than encryption of AES 256, as well as better performance of computational cost as compared to homomorphically encrypted AES. As stated by previous research, this is in agreement with the finding of previous research that AI-enhanced encryption reduced latency without compromising data integrity (Camacho, 2024). It is also worth mentioning that the AI-driven threat intelligence systems using NLP and reinforcement learning came with as much as 96.5% accuracy in cybersecurity monitoring (Familoni, 2024), thereby cutting down the false positive rates of security systems.

One of the major positive aspects of the study notes from this study was the robustness of security frameworks that sit on top of federated learning against adversarial AI attacks. Also, Federated Learning's 8.5% can also be a good reason for arguing the reliability of countering adversarial threats compared to Autoencoders 8.5% and XGBoost's 11.8%. Similar research has found that a differential privacy strategy with adversarial training is a good way to improve cybersecurity resilience (Mbah & Nkechi, 2024). But, in this case, the use of AI in cybersecurity involves many challenges, such as hostile AI attacks, regulatory compliance, bias in AI models, and so on. To have cybersecurity systems trusted and governed, they need to be deployed and governed ethically. Thus, finally, regulatory frameworks such as GDPR, NIST, ISO 27001, and so on, are likely to fill in part of these gaps by the use of explainable AI (XAI) models (Akhtar & Rawol, 2024). The work contributes to the advancement of AI-integrated cybersecurity systems on improving threat intelligence performance, encryption, and accuracy. It offers a scalable and flexible cybersecurity solution to MNCs, with CSI features of the Federated Learning, CNN-LSTM Hybrid models, and AI-enhanced encryption working together. The research that should be done to solve global cybersecurity is around regulatory compliance, AI bias reduction, and the implementation of AI cybersecurity in the real world.

Comparison with Recent Studies

The table below compares this study with other recently conducted research on AI-driven cybersecurity frameworks, highlighting differences in approach, methodology, and key findings.

Table 5: Comparison of This Study with Recent AI-Driven Cybersecurity Research

Study	AI Model Used	Accuracy (%)	Adversarial Robustness	Encryption Efficiency	Threat Intelligence Performance
This Study	Federated Learning, CNN-LSTM Hybrid	**99.0**	**8.5% attack success rate** (lowest)	**2.5% encryption overhead (lowest)**	**96.5% accuracy, 5.1% false positive rate**
Çakır (2024)	Deep Learning IDS	97.3	12.2%	3.8%	93.1% accuracy
Shoetan *et al.*, (2024)	Reinforcement Learning	96.2	14.5%	4.2%	92.4% accuracy
Ovabor *et al.*, (2024)	NLP-Based AI	95.8	17.1%	5.1%	91.3% accuracy
Camacho (2024)	AI-Optimized AES	94.5	19.6%	**2.7%**	90.2% accuracy
Familoni (2024)	XGBoost IDS	92.7	11.8%	5.3%	89.7% accuracy
Kulothungan (2024)	Hybrid AI Framework	91.2	**8.9%**	4.5%	88.3% accuracy

VIII. CONCLUSION

This research shows the significance of cybersecurity frameworks fueled by AI in helping multinational companies (MNCs) detect threats, make their encryption more secure, and minimize adverse responses. The results show that the accuracy of the Intrusion Detection (99.0%) and the reaction time (120 ms) using CNN-LSTM Hybrid and Federated Learning models are very superior to the conventional machine learning models. An artificial intelligence (AI)-driven threat intelligence system via reinforcement learning and natural language processing (NLP) is capable of reducing false positives as well as enhancing the detection hitting rate (96.5%) in the context of real-time cyber threat mitigation. AI-encrypted AES and Zero Trust Architecture (ZTA) have 2.5 percent of the cost of encryption and can be highly beneficial in the encryption of MNC infrastructures on a large scale. Furthermore, Federated Learning-based models show resilience against adversarial attacks, where they achieve the best attack success rate (8.5%) as compared to other AI methods. While there has been much progress towards AI-driven cybersecurity solutions, and indeed, there have been so many barriers on the way to progress, like AI bias, regulatory compliance, and even hostile AI attacks. In particular, for GDPR, ISO 27001, NIST, and XAI standards building and ethical use cases of AI, we need. The results of this study indicate that the federated security strategy used is superior to the majority of the existing AI-based cybersecurity frameworks and are presented further in the comparison between the proposed system and previously studied research. It demonstrates that AI-integrated security models are feasible and how AI-integrated security solutions work in large multinational corporations. There is further research to be done improving future AI governance frameworks, implementing AI that can incorporate post-quantum cryptography, and a consideration of any ethical implications regarding AI. The AI-driven security frameworks will continue to be very crucial as frameworks develop in the use of AI to improve global cybersecurity resilience and protect digital infrastructure against new cyber threats.

REFERENCES

- Prabhakar, S., Nalinaksha, I., & Anjaneyulu, V. (2023). Role of AI in enhancing cybersecurity measures to protect sensitive financial data. International Journal of Science and Research Archive. DOI: 10.30574/ijsra.2023.10.1.0700
- Mbah, G. O., & Nkechi, A. (2024). AI-powered cybersecurity: Strategic approaches to mitigate risk and safeguard data privacy. World Journal of Advanced Research and Reviews. DOI: 10.30574/wjarr.2024.24.3.3695
- Moore, C. (2025). AI-powered big data and ERP systems for autonomous detection of cybersecurity vulnerabilities. SSRN Electronic Journal. DOI: 10.2139/ssrn.5114902
- Adeyeye, O. J., Akanbi, I., Emeteveke, I., & Emehin, O. (2024). Leveraging secured AI-driven data analytics for cybersecurity: Safeguarding information and enhancing threat detection. International Journal of Research Publication and Reviews. DOI: 10.55248/gengpi.5.1024.2911
- Wang, R. (2023). AI use in enhancing cybersecurity for safeguarding digital information. 2023 International Conference on Applied Physics and Computing (ICAPC). DOI: 10.1109/ICAPC61546.2023.00082
- Ilieva, R., & Stoilova, G. (2024). Challenges of AI-driven cybersecurity. 2024 XXXIII International Scientific Conference Electronics (ET). DOI: 10.1109/ET63133.2024.10721572
- Dandamudi, S. R. P., Sajja, J., & Khanna, A. (2025). AI transforming data networking and cybersecurity through advanced innovations. International Journal of Innovative Research in Computer Science and Technology. DOI: 10.55524/ijircst.2025.13.1.6

- Çakır, A. M. (2024). AI Driven Cybersecurity. *Human Computer Interaction.* DOI**:** 10.62802/jg7gge06
- Shoetan, P. O., Amoo, O. O., Okafor, E. S., & Olorunfemi, O. L. (2024). Synthesizing AI's Impact on Cybersecurity in Telecommunications: A Conceptual Framework. *Computer Science & IT Research Journal.* DOI: 10.51594/csitrj.v5i3.908
- Ovabor, K., Sule-Odu, I. O., Atkison, T., Fabusoro, A. T., & Benedict, J. O. (2024). AI-driven threat intelligence for real-time cybersecurity. *Open Access Research Journal of Science and Technology.* DOI**:** 10.53022/oarjst.2024.12.2.0135
- Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science.* DOI**:** 10.60087/jaigs.v3i1.75
- Familoni, B. T. (2024). Cybersecurity Challenges in the Age of AI. *Computer Science & IT Research Journal.* DOI**:** 10.51594/csitrj.v5i3.930
- Kulothungan, V. (2024). Securing the AI Frontier: Ethical and Regulatory Imperatives. *IEEE International Conference on Big Data.* DOI**:** 10.1109/BigData62323.2024.10826010.