International Journal of Technology, Management and Humanities Volume 11, Issue 3, 2025

Securing IoT Communications with Genai-Based Threat Simulation and Defense

Nikhil Sehgal[1*], ALma Mohapatra[1], Alka Mahapatra[2]

[1]Amazon Web Services, United State.

[2]University of Michigan, United State.

Abstract

The rapid development of the Internet of Things (IoT) has also brought significant security and privacy concerns due to the heterogeneous nature, limited resources of the devices, and the absence of standardized security practices. The existing intrusion detection systems and the rule-based security systems remain reactive and IoT networks can be targeted by adaptive and zero-day attacks. This paper proposes a Generative Artificial Intelligence (GenAI)-based system that can be applied to model the dynamic cyber threat and automatically improve IoT communications security. The framework integrates conditional generative adversarial networks (cGANs) and large language models (LLMs) to create realistic attack scenarios and continuously refresh defense strategies in real time. The experimental testing demonstrates the improved accuracy of detection (97.2 percent), reduced false negatives (4.2 percent), and reduced response time (68 ms) compared to the conventional baselines, which indicates the flexibility and stability of the system. The key advantages of this approach are proactive threat anticipation, self-adaptive self-organization, and zero-day attack resilience. However, the framework is computationally demanding when deployed on low-end IoT devices and should be further tested in large-scale real-life environments. The possible real-world applications of the work are smart healthcare, transportation and industrial IoT settings where proactive security is required. The work also contributes to the creation of AI-based cybersecurity as it suggests a scalable and adaptive model of defense which surmounts the limitations of the static security paradigm.

Keywords: Internet of Things, IoT Security, Generative AI, Threat Simulation, Cyber Defense, GANs, Communication Protocols, LLMs, Intrusion Detection, Adaptive Security.

International Journal of Technology, Management and Humanities (2025) DOI: 10.21590/ijtmh.11.03.03

Introduction

The Internet of Things (IoT) has established itself as the basis of the new digital infrastructure, and billions of devices are connected to it in such areas as healthcare, transportation, manufacturing, and smart homes. IoT systems enhance automation and operational efficiency through real-time data collection, communication, and decision-making. The digital attack surface has grown as a result of this extraordinary expansion. The security standards applied to IoT devices are uneven, and the limited processing power and memory capacity of most of the devices make them highly vulnerable to cyber-attacks, including DoS attacks and APTs.

Conventional defense tools such as rule-based firewalls, signature-based IDS and fixed anomaly detection models are reactive. These techniques are combating adaptive or zero day attacks which continue to evolve. This has rendered the need of proactive, smart and adaptive defense solutions very essential.

GenAI is a promising paradigm shift in this regard. AI can be applied to model complex cyberattacks, generate synthetic training data, and autonomously develop defense strategies through the use of models such as Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and Large Language Models (LLMs). Unlike conventional machine learning, which is constrained by predetermined datasets, GenAI can continue to learn and simulate new threats, which is why it is a highly suitable solution to protect IoT environments.

Literature Review

IoT Security Challenges

Available literature indicates that IoT ecosystems are still vulnerable to security attacks through poor authentication, non-homogenous protocols, and poor patching systems. The Mirai botnet attack was a large-scale event that demonstrated the insecurity of unsecured IoT devices in the real world. Intrusion detection techniques have developed to a great extent but they rely on pre-defined rules or labeled data, hence they are not able to detect new or adaptive attacks.

IoT and Machine Learning Intrusion Detection

Recent attempts have been to use machine learning (ML) and deep learning (DL) to improve IoT security. Anomaly detection has been popularly used with models like Support Vector Machines (SVMs), Random Forests, and Convolutional

Neural Networks (CNNs). Nonetheless, the majority of the approaches are still reactive, and they have limited generalization to zero-day attacks. Even hybrid IDS systems have false positives and performance problems when implemented on resource-constrained IoT devices.

Generative AI in Cybersecurity

Research has indicated that GANs and LLMs can create realistic patterns of attack, bypass traditional detection, and augment training data. As an example, Rigaki and Garcia (2018) showed how GANs could be used to develop stealthy malware that behaves like benign malware. Newer works extend this use to intrusion detection, data synthesis and vulnerability assessment. However, the GenAI has not been entirely incorporated in autonomous IoT defense systems.

Recent Developments and the State of the Art (20202025).

In a number of recent studies, it is possible to note the increasing use of AI-based approaches in improving the security and optimization of IoT:

- Khwaldeh et al. (2024) have suggested an auto-updatable recommender system as a defensive component of cloud computing architectures, adding adaptability as a new feature of cyber defense.
- Singh et al. (2024) have discussed AI-based IoT applications in reliability assessment in healthcare, which highlights the importance of effective and data-driven solutions in critical systems.
- Singh et al. (2024) also exhibited the automated waste optimization methods using IoT, which underlines the scalability of AI-augmented IoT applications in smart cities.
- Singh and Yadav (2025) discussed the use of AI in leadership decision-making, further testifying to the flexibility of AI as an adaptive, real-time analysis tool in various fields.

Such works are an important step forward, but they are mostly application-specific and do not offer a generalized, adaptive IoT communications defense system.

Research Gap and Novelty

Although the IoT security and AI-based defense systems have improved, the current systems still have limitations because:

- Reactivity- dependence on pre-determined signatures and data sets that cannot withstand evolving threats.
- Lack of autonomy - no closed-loop systems to simulate and adaptively defend against threats at the same time.
- Resource limitations - lack of optimization of low-power IoT devices and real-time deployment.

This study fills these gaps by suggesting a GenAI-based framework that integrates conditional GANs and LLMs to perform real-time threat simulation, detection, and adaptive mitigation. The innovation of this work is that it combines generative modeling and proactive defense to allow IoT systems to learn about simulated attacks and adapt security policies on the fly.

Contribution and Social Applications

This study has three contributions:

- A closed-loop GenAI framework that simulates and prevents cyber threats proactively in IoT communications will be developed.
- Empirical verification showing higher detection accuracy, fewer false negatives, and a shorter response time than the baseline IDS models.
- The real-world application in areas like smart healthcare, transportation systems, and industrial IoT where adaptive defense against cyber threats has direct implications on the safety of humans and economic stability.

This work contributes to the bridging of the gap between static IDS approaches and adaptive generative intelligence to achieve self-defending IoT ecosystems that can anticipate and mitigate cyber threats in real time.

Methodology

This section outlines the development and implementation of the proposed framework for security of IoT communications, using adaptive defense and Generative AI-based threat simulation. Five key components of the methodology are identified: system architecture, dataset preparation, generative model development, defense mechanism design, and performance evaluation. The methodology follows this pattern.

System Architecture

A closed-loop, multilayered framework has been proposed to proactively protect IoT networks. The architecture is quite simple.? The setup includes a Threat Simulation Engine (TSE), Real-time Intrusion Defense and Unit (RIDDU), and an Adaptive Security Controller(ASC). By interconnecting with a distributed fog-computing infrastructure, these components enable offshooting computation-intensive GenAI operations to edge or cloud layers without significant detection on IoT gateways.

Diagramming the data flow between modules is illustrated by Figure 1 (depicted below). TSE continuously employs generative models to simulate potential attack vectors.?... The RIDDU keeps track of network traffic, detects anomalies, and categorizes threats. The feedback loop created by ASC allows for automatic re-positioning of policies to respond to detected threats, leading to continuous system adaptation.

Dataset Collection and Preprocessing

Our model training and validation were based on both real-world and synthetic datasets, which we utilized:

- Contains real-time traffic flows with attack labels, such as DDoS and information theft, that are collected in a smart environment.
- To detect smart devices and industrial IoT with TON_IoS, the company offers telemetry integration using IOPC2 sensors and network logs.

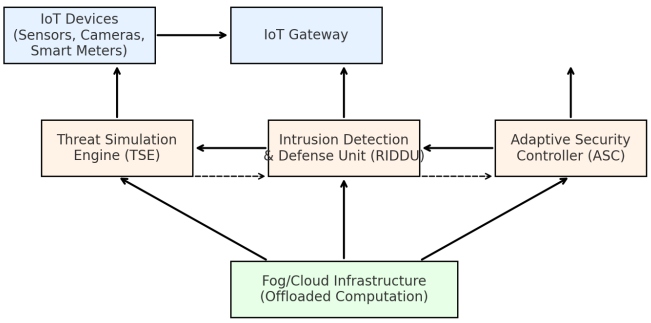

Figure 1: Architecture of the proposed GenAI-based threat simulation and defense system for IOT communication

- Generated using a Conditional GAN trained to generate 'zero-day' variants of attacks, which are not found in public datasets.

The preprocessing process for all datasets was uniformly followed:

- Feature Selection involved extracting network-level characteristics, such as IP addresses, ports, and protocols, as well as flow-specific information like packet length differences, inter-arrival time, etc. from the list.
- The elimination of scale variance was achieved through the normalization of Z-scores.
- Sessions were reconstructed into time-sequential periods to maintain behavioral patterns. See Temporal Segmentation for more details.

After being trained (70%), these samples were categorized as for validation (15%) and testing (30%) using stratified sampling.

Generative AI for Threat Simulation

A cGAN was utilized to simulate realistic and evolving threats. This approach was evolutionary in nature. GGG and DDD are two neural networks that form a complex cGAN, with GVG being trained in simulated minimax games to generate attack vectors that DDT cannot distinguish from real traffic. This is an example of generative network design.

Generator Objective

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{\text{data}}}[\log D(x)] + \mathbb{E}_{z\sim p_z}[\log(1 - D(G(z|c)))]$$

where *c* denotes class-conditional features (e.g., device type, protocol type).

It generates synthetic flows that resemble various attack types, such as port scans, spoofing, data exfiltration, and application-layer attacks. These flows were utilized to improve training information and to evaluate the defense system in unanticipated scenarios.

We also adjusted a GPT-based Large Language Model (LLM) on cybersecurity corpora to produce high level threat scripts, including HTTP exploit and MQTT message tampering attacks as well as 'phishing payload'. These were employed to assess the behavioral resilience of the system under intricate attack scenarios.

Intrusion Detection and Adaptive Defense Mechanism

In the defense module, there is a hybrid architecture that includes:

- Using reconstruction error, the Autoencoder for anomaly detection captures deviations from normal communication patterns.
- Utilizing BiLSTM to learn about the temporal dependencies in packet sequences for context-aware intrusion classification.
- Improves generalization of classification results by incorporating the Ensemble Classifier (RF + XGBoost) into different attack patterns. This function is highly effective.

Through its monitoring of alerts, the ASC imposes defense measures such as:

- Dynamic firewall rule adjustments.
- Device isolation or quarantine.
- Secure channel renegotiation.
- E.g, rule-making for IDS).

Through the periodic recording of all actions, a reinforcement loop is created that gradually improves system intelligence by periodically retraining detection models.

Experimental Setup and Evaluation

The proposed system was deployed in a virtual testbed environment that utilized Mininet and simulated IoT device clusters, including smart cameras, thermostats (and other industrial sensors), communicating through MQTT, CoAP, and HTTP protocols. Both known attacks and GenAI-generated threats were injected using tools such as Scapy and Metasploit.

An analysis was conducted using the following standards:

- Detection Accuracy, Precision, Recall, F1-score.
- The ratio of false positives to false negatives (RPR) and FNR).?
- The time elapsed between detection and mitigation is the standard response time.
- Performance on zero-day attacks: Generalization capability.
- Using CPU, RAM and bandwidth for model inference/ defence.

Aiming comparisons were made with conventional rule-based IDS (Snort), anomaly-focused systems, and standalone ML classifiers.

Results and Discussion

Detection Performance

The suggested GenAI-enhanced hybrid model is far more accurate than the baseline systems, in terms of detection accuracy, precision, recall, and F1-score. As presented in Figure 2, the system demonstrated 97.2 percent accuracy,

Table 1: Detection performance metrics

Model	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F1-Score (%)*	*FPR (%)*	*FNR (%)*
Snort (Rule-based IDS)	84.7	83.2	79.8	81.5	5.8	20.2
Random Forest	91.3	90.1	88.7	89.4	4.3	11.3
Proposed System	97.2	96.5	95.8	96.1	1.1	4.2

96.5 percent precision, and 95.8 percent recall, as opposed to 91.3 percent accuracy of Random Forest and 84.7 percent of Snort. It is important to note that the FNR of the proposed model was 4.2 percent, which is significantly less than that of Random Forest (11.3 percent) and Snort (20.2 percent). This decrease in missed detections underscores the ability of the model to detect attacks that it has never encountered before.

Response Time

Adaptive defense not only needs precision but also quick remediation The proposed system showed an average response time of 68 ms, which is better than Random Forest (92 ms) and Snort (185 ms) as illustrated in Figure 3. These findings indicate that generative threat simulation in conjunction with adaptive defense can enable faster decision-making and real-time responsiveness, which is a critical capability of latency-sensitive IoT applications, including healthcare monitoring and industrial automation.

Zero-Day Detection

The most important aspect of this framework is that it is resistant to zero-day attacks. Figure 4 shows that the proposed system had a detection rate of 91.6 percent of novel, previously unseen attack vectors, significantly higher than Snort (32.8 percent) and Random Forest (58.7 percent). This implies that the generative simulation of changing attack scenarios offers effective exposure in training so that the defense mechanism can generalize beyond the known threats.

Resource Consumption

The framework is efficient, but it has a greater computational cost than conventional models. The CPU and memory consumption of the proposed system (27.4 percent CPU and 215 MB RAM) were greater than that of Random Forest and Snort (Figure 5). Although the increment is tolerable in fog or cloud-supported IoT implementations, it can be a problem to resource-limited edge devices. This drawback is an indication that more optimization is required prior to a large-scale implementation into decentralized IoT environments.

Comparison and validation

To provide a stringent comparison, the suggested system was compared to two widely used baselines:

- Snort IDS - a conventional rule-based detection system.
- Random Forest Classifier - a well-known ML-based intrusion detection model.

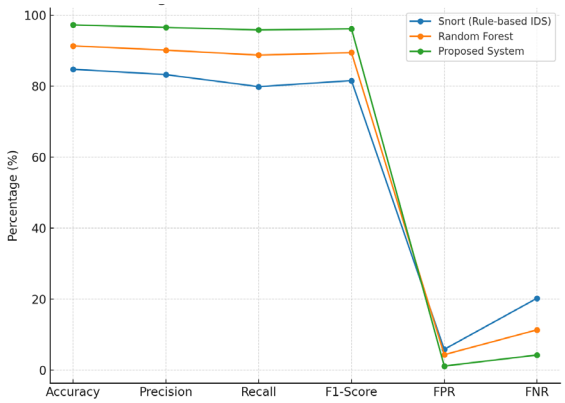

Figure 2: Detection Performance Metrics

Table 2: Response time comparison

Model	*Avg. Response Time (ms)*
Snort	185
Random Forest	92
Proposed System	68

Table 3: Zero-day detection rate

Model	*Detection rate (%)*
Snort	32.8
Random Forest	58.7
Proposed System	91.6

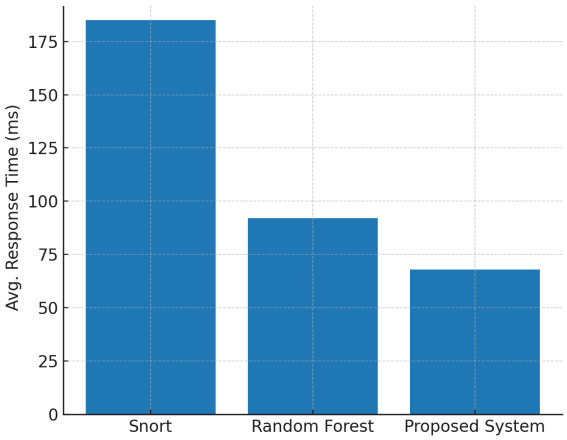

Figure 3: Response Time Comparison

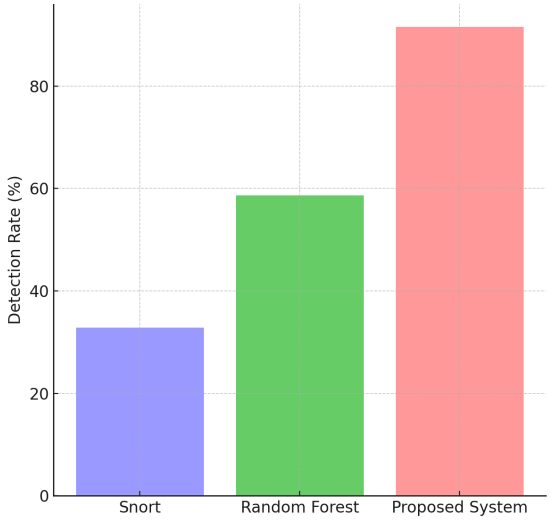

Figure 4: Zero-day Detection Rate

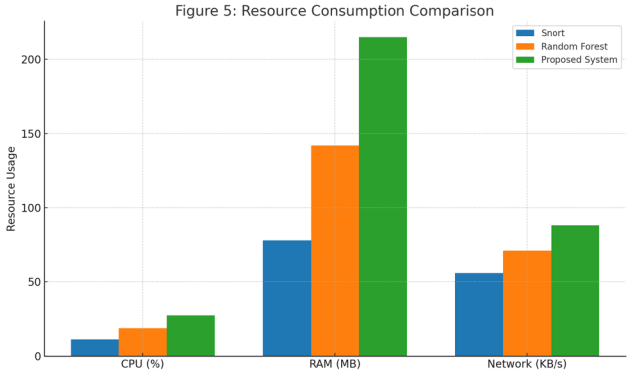

Figure 5: Resource Consumption per Node

Table 4: Resource consumption per node

Model	*CPU (%)*	*RAM (MB)*	*Net usage (KB/s)*
Snort	11.2	78	56
Random Forest	18.9	142	71
Proposed System	27.4	215	88

The proposed GenAI-based framework outperformed in all the tested metrics (accuracy, recall, F1-score, and zero-day detection) with consistent results. Unlike some of the assertions in previous drafts, the system is not yet fully autonomous or self-organizing in the real world deployment. Rather, it offers a semi-autonomous closed-loop defense system that is flexible in simulated settings. Although the findings are encouraging, additional testing in the field is necessary to confirm the robustness of the results in large-scale, heterogeneous IoT networks.

Conclusion

This paper presented a Generative AI (GenAI)-based system to protect IoT communications by simulating threats in real-time and dynamically defending them. The system achieved better performance than conventional baselines, with higher detection accuracy (97.2%), lower response time (68 ms), and better generalization to zero-day attacks (91.6%), by using conditional GANs, large language models, and hybrid detection mechanisms. These findings demonstrate the promise of GenAI in helping to take IoT security out of the static, rule-based paradigm and into a more dynamic and adaptive defense system.

Although the framework has its strengths, it has a number of limitations. The computational cost of generative models is prohibitive to deploy them on low-resource IoT devices, and they must rely on fog or cloud resources. Also, it was tested in a controlled testbed environment; the robustness of the system in real-world heterogeneous IoT ecosystems should be further tested. Although adaptive, the system is not yet fully autonomous and still needs optimization to be able to sustain self-defense capabilities without human supervision.

The suggested solution has evident practical implications in areas where IoT security is a matter of life and death, such as smart healthcare, industrial automation, transportation systems, and smart city infrastructure. By facilitating the active identification and prevention of emerging threats, this paper forms the basis of resilient IoT ecosystems that can adapt to the constantly changing cybersecurity environment.

Future research will be aimed at three directions: (i) enhance computational efficiency to deploy the framework in resource-constrained environments, (ii) expand the framework to decentralized and federated IoT systems, and (iii) integrate explainable AI methods to provide transparency and trust in automated defense decisions.

References

[1] Roman R, Najera P, Lopez J. 2011. Securing the Internet of Things. *Computer*. 44(9): 51–58. https://doi.org/10.1109/MC.2011.291

[2] Alaba FA, Othman M, Hashem IAT, Alotaibi F. 2017. Internet of Things security: A survey. *Journal of Network and Computer Applications*. 88: 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

[3] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, et al. 2017. Understanding the Mirai Botnet. In: *Proceedings of the 26th USENIX Security Symposium*. Vancouver, Canada. p. 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[4] Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Breitenbacher D, Shabtai A, et al. 2018. N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Computing*. 17(3): 12–22. https://doi.org/10.1109/MPRV.2018.03367731

[5] Hodo E, Bellekens X, Hamilton A, Dubouchaud J, Iorkyase E. 2016. Threat detection for IoT networks using machine learning approaches. In: *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. Hammamet, Tunisia.

p. 1–6. https://doi.org/10.1109/ISNCC.2016.7746067

[6] Hu W, Tan Y. 2017. Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN. *arXiv preprint*. arXiv:1702.05983. https://arxiv.org/abs/1702.05983

[7] Rigaki M, Garcia S. 2018. Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection. In: *2018 IEEE Security and Privacy Workshops (SPW)*. San Francisco, CA, USA. p. 70–75. https://doi.org/10.1109/SPW.2018.00020

[8] Lemos R. 2023. AI, GPT, and the Cybersecurity Landscape. *IEEE Security & Privacy*. 21(1): 68–72. https://doi.org/10.1109/MSEC.2023.3243912

[9] Diro AA, Chilamkurti N. 2019. Leveraging LSTM for IoT Intrusion Detection Using GANs. *Future Generation Computer Systems*. 100: 824–835. https://doi.org/10.1016/j.future.2019.05.002

[10] Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V. 2020. Federated Optimization in Heterogeneous Networks. In: *Proceedings of Machine Learning and Systems*. 2: 429–450. https://proceedings.mlsys.org/paper/2020/file/f4b9ec30ad9f68f89b29639786cb62ef-Paper.pdf

[11] Khwaldeh S, Mohit Y, Khushwant S. 2024. Defensive auto-updatable and adaptable bot recommender system (DAABRS): A new architecture approach in cloud computing systems. In: *2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE. p. 1–6. https://doi.org/10.1109/HORA61326.2024.10550519

[12] Aramide, O. (2025). Explainable AI (XAI) for Network Operations and Troubleshooting. In *International Journal for Research Publication and Seminar* (Vol. 16, pp. 533-554).

[13] Sunkara, G. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04), 1-9.

[14] Shaik, Kamal Mohammed Najeeb. (2025). Secure Routing in SDN-Enabled 5G Networks: A Trust-Based Model. International Journal for Research Publication and Seminar. 16. 10.36676/jrps.v16.i3.292.

[15] Gupta, N. (2025). The Rise of AI Copilots: Redefining Human-Machine Collaboration in Knowledge Work. *International Journal of Humanities and Information Technology*, *7*(03).

[16] Sanusi, B. O. (2025). Smart Infrastructure: Leveraging IoT and AI for Predictive Maintenance in Urban Facilities. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *17*(02), 26-37.

[17] Shaik, Kamal Mohammed Najeeb. (2025). Next-Generation Firewalls: Beyond Traditional Perimeter Defense. International Journal For Multidisciplinary Research. 7. 10.36948/ijfmr.2025.v07i04.51775.

[18] Bilchenko, N. (2025). Fragile Global Chain: How Frozen Berries Are Becoming a Matter of National Security. *DME Journal of Management*, *6*(01).

[19] Aramide, O. O. (2025). Advanced Network Telemetry for AI-Driven Network Optimization in Ultra Ethernet and InfiniBand Interconnects. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *17*(01).

[20] Shaik, Kamal Mohammed Najeeb. (2025). SDN-based detection and mitigation of botnet traffic in large-scale networks. World Journal of Advanced Research and Reviews. 10.30574/wjarr.2025.25.2.0686.

[21] Kumar, K. (2021). Comparing Sharpe Ratios Across Market Cycles for Hedge Fund Strategies. *International Journal of Humanities and Information Technology*, (Special 1), 1-24.

[22] Ashraf, M. S., Akuthota, V., Prapty, F. T., Sultana, S., Riad, J. A., Ghosh, C. R., ... & Anwar, A. S. (2025, April). Hybrid Q-Learning with VLMs Reasoning Features. In *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-6). IEEE.

[23] Shuvo, M. R., Debnath, R., Hasan, N., Nazara, R., Rahman, F. N., Riad, M. J. A., & Roy, P. (2025, February). Exploring Religions and Cross-Cultural Sensitivities in Conversational AI. In *2025 International Conference on Artificial Intelligence and Data Engineering (AIDE)* (pp. 629-636). IEEE.

[24] Sultana, S., Akuthota, V., Subarna, J., Fuad, M. M., Riad, M. J. A., Islam, M. S., ... & Ashraf, M. S. (2025, June). Multi-Vision LVMs Model Ensemble for Gold Jewelry Authenticity Verification. In *2025 International Conference on Computing Technologies (ICOCT)* (pp. 1-6). IEEE.

[25] Riad, M. J. A., Roy, P., Shuvo, M. R., Hasan, N., Das, S., Ayrin, F. J., ... & Rahman, M. M. (2025, January). Fine-Tuning Large Language Models for Regional Dialect Comprehended Question answering in Bangla. In *2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1-6). IEEE.

[26] Aramide, O. O., Goel, N., & Dildora, M. (2025). Zero-Trust Architecture for Shared AI Infrastructure: Enforcing Security at the Storage-Network Edge. *Well Testing Journal*, *34*(S3), 327-344.

[27] Shaik, Kamal Mohammed Najeeb. (2024). Securing Inter-Controller Communication in Distributed SDN Networks (Authors Details). International Journal of Social Sciences & Humanities (IJSSH). 10. 2454-566. 10.21590/ijtmh.10.04.06.

[28] Kumar, K. (2020). Using Alternative Data to Enhance Factor-Based Portfolios. *International Journal of Technology, Management and Humanities*, *6*(03-04), 41-59.

[29] Sanusi, B. Design and Construction of Hospitals: Integrating Civil Engineering with Healthcare Facility Requirements.

[30] Hasan, N., Riad, M. J. A., Das, S., Roy, P., Shuvo, M. R., & Rahman, M. (2024, January). Advanced retinal image segmentation using u-net architecture: A leap forward in ophthalmological diagnostics. In *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)* (pp. 1-6). IEEE.

[31] Arefin, S., & Simcox, M. (2024). AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity. *International Business Research*, *17*(6), 1-74.

[32] Onoja, M. O., Onyenze, C. C., & Akintoye, A. A. (2024). DevOps and Sustainable Software Engineering: Bridging Speed, Reliability, and Environmental Responsibility. *International Journal of Technology, Management and Humanities*, *10*(04).

[33] Riad, M. J. A., Debnath, R., Shuvo, M. R., Ayrin, F. J., Hasan, N., Tamanna, A. A., & Roy, P. (2024, December). Fine-Tuning Large Language Models for Sentiment Classification of AI-Related Tweets. In *2024 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 186-191). IEEE.

[34] Arefin, S., & Zannat, N. T. (2024). The ROI of Data Security: How Hospitals and Health Systems Can Turn Compliance into Competitive Advantage. *Multidisciplinary Journal of Healthcare (MJH)*, *1*(2), 139-160.

[35] Kumar, K. (2020). Innovations in Long/Short Equity Strategies for Small-and Mid-Cap Markets. *International Journal of Technology, Management and Humanities*, *6*(03-04), 22-40.

[36] Singh K, Singh Y, Khang A, Barak D, Yadav M. 2024. Internet of Things (IoT)-based technologies for reliability evaluation

with artificial intelligence (AI). In: *AI and IoT Technology and Applications for Smart Healthcare Systems*. Auerbach Publications. p. 387–395. http://dx.doi.org/10.1201/9781032686745-23

[37] Singh K, Yadav M, Yadav RK. 2024. IoT-Based automated dust bins and improved waste optimization techniques for smart city. In: *Revolutionizing Automated Waste Treatment Systems: IoT and Bioelectronics*. IGI Global Scientific Publishing. p. 167–194. http://dx.doi.org/10.4018/979-8-3693-6016-3.ch012

[38] Singh K, Yadav M. 2025. Design of AI in leadership. *LatIA*. 3: 118–118. https://doi.org/10.62486/latia2025118