International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1336-1342
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0190

Threat Intelligence Platform Empowered by Generative Ai with Quantum-Security

DR. K. Maharajan[1], Mugeshwaran K[2], Dumala Nithish[3], Dinesh S[4], Uday N[5]

[1]Associate professor, Dept. of CSE, Kalasalingam Academy of Research and Education., Virudhunagar, Tamil Nadu, India.

[2,3,4,5]UG Scholar, Dept. of CSE, Kalasalingam Academy of Research and Education., Virudhunagar, Tamil Nadu, India.

Emails ID: *maharajank@gmail.com[1], Mugesh.edu@gmail.com[2], reddynithsh042@gmail.com[3], Saravanandinesh9876@gmail.com[4], udaynaredla06@gmail.com[5]*

Abstract

The rapid evolution in types of cyber threats and anticipated threats through quantum computing requires a change in cybersecurity strategy. The traditional Threat Intelligence Platforms (TIPs) usually use static rule-based systems and reactive measures to provide real-time solutions to address attacks that are either emerging or sophisticated. This paper proposes a next-generation Threat Intelligence Platform (TIP) incorporating Generative Artificial Intelligence (GenAI) to enable predictive threat scenario modelling, anomaly detection, and autonomous mitigation strategies using quantum-security mechanisms to provide very-long-term cryptographic resilience. The GenAI engine provides live threat simulation, adequate situational awareness, and improved anomaly detection accuracy by large-scale cyber datasets. At the same time, the Quantum-Security Module consists of post-quantum cryptographic (PQC) algorithms, such as lattice-based, hash-based, and multivariate cryptosystems. All of these seek to plug holes caused by quantum adversaries. The suggested TIP architecture is a multi-layered one that possesses a data ingestion layer, an AI-driven threat analytics, a quantum-resilient cryptographic framework, and an interactive visualization dashboard. It delineates an architectural framework, important points of innovation, and potential applications across the main sectors of finance, healthcare, defence, and enterprise cybersecurity. Additionally, the research presents a high-level strategic roadmap for the deployment of GenAI-intensified TIPs with quantum-resilient security, scalable and adaptable for future-proof data integrity. Addressing AI-enabled predictive security features and post-quantum cryptographic resilience, the research offers future-proof cybersecurity as an answer to continuous changes in digital threats.

Keywords: *Threat Intelligence Platform (TIP), Generative AI, AI-driven Security Analytics, Generative Adversarial Networks (GANs), Quantum Security.*

1. Introduction

The digital landscape is evolving, with cyber threats becoming increasingly sophisticated and complex. Advanced Persistent Threats (APTs), zero-day vulnerabilities, ransomware campaigns, and AI-driven attacks are quickly proliferating across organizations of various sizes and sectors. Traditional Threat Intelligence Platforms (TIPs) primarily rely on static rules, signature-based detection, and manually curated intelligence feeds, which sometimes insufficiently address emerging threat vectors that evolve in real-time [12]. The imminent threat posed by quantum computing intensifies the cybersecurity landscape. Traditional public key cryptography systems, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), which depend on complex mathematical problems for their security, are vulnerable to quantum algorithms like Shor's algorithm. Without quantum-resistant cryptographic safeguards, firms are vulnerable to significant data breaches and systemic vulnerabilities from adversaries with quantum computing capabilities. This research introduces an innovative Threat Intelligence Platform (TIP) that integrates Generative Artificial Intelligence (GenAI) with quantum-resistant security measures. This research aims to establish a multi-layered TIP architecture that incorporates AI-driven threat analytics and quantum-resilient cryptography, develop a framework for predictive threat modeling and anomaly detection using GenAI, and devise a strategic roadmap for implementing scalable and adaptable quantum-secure cybersecurity measures to guarantee future-proof data integrity. The proposed platform employs GenAI to simulate cyber threats, predict attack patterns, and enhance real-time anomaly detection. The technology utilizes AI-driven threat modeling to proactively discover new attack vectors while minimizing false positives [11]. This AI platform is augmented with quantum-resistant cryptographic techniques, including lattice-based encryption, hash-based signatures, and multivariate schemes, to protect sensitive data from both traditional and quantum attacks [6]. This integrated system represents a fundamental transition from conventional reactive cybersecurity approaches to proactive threat intelligence, allowing enterprises to foresee and avert cybersecurity problems while adjusting to emerging hurdles in quantum technology. This paper outlines an architectural framework, innovations, and applications that provide fundamental principles for developing flexible and resilient cybersecurity systems designed for an increasingly volatile digital landscape [12].

2. Background and Motivation

2.1 Cybersecurity Challenges in the Modern Era

The building of the digital infrastructure happens very quickly which makes the attack surfaces to be more open to cyber threats. Advanced Persistent Threats (APTs), zero-day exploits, ransomware, and state-sponsored cyber warfare continue to evolve, bypassing traditional security defensive Conventional Threat Intelligence Platforms (TIPs) mainly depend on signature-based detection, rule-based analysis, and historical threat intelligence, which frequently fail to detect the novel or adaptive attack strategies. In addition to this, the rising complexity of IT environments comprising cloud computing, IoT, and remote work ecosystems asks for a more dynamic and predictive approach to the threat intelligence.

2.2 The Quantum Computing Threat

Before diving into the text-to-speech technology presently forming, we should observe the history, the elementary and fundamental notions, and the macro methods that make it achievable. Dealing with countless theoretical aspects and practical issues, cryptography generally appears as an enigma. Nevertheless, analyzing its grinding wheels can be a good starting point. By far, RSA and ECC algorithms are the ones behind the encryption standards, which are prone to Shor's algorithm being able to factorize most of the random numbers and crash the asymmetric cryptographic keys. Particularly, companies need to adopt a quantum-resistant data protection infrastructure and to secure themselves from future cyber-attacks and then adopt post-quantum cryptography (PQC) systems. In the coming changes of paradigms, it is perhaps in the area of cryptography where the most visible symptoms of Quantum Computing (QC) will be the first seen and at the same time a Salient part of it, it will be. Otherwise, no new progress can be seen, and it will be a matter of concern to our stakeholders. Firstly, sensitive communications, banking transactions, and secure data are at risk [1][3].

2.3 Generative AI in Cybersecurity

Generative AI (GenAI) is a technology that is mostly known for using Cybersecurity for threat detection, predictive analytics and automating incident responses. This is done by creating a deep learning model such as Generative Adversarial Networks (GANs) and architectures such as transformer-based architectures (e.g., GPT) which is the father of Deep learning the advantages of them are that of the following.

- Cybersecurity teams can examine proactive countermeasures and check the security of their systems by simulating complex attack scenarios as the method is effective[2].

- ML-based security models can be trained on synthetic but lifelike datasets to fundamentally change the approach of security and reduce the need for real-world data that is limited.
- For example, it can examine and learn how normal activities are done. Hence, repairs can be made easier and faster as problems are well diagnosed. It can also check for issues and a discussion by comparing security systems that are similar which is very accurate.

On the other hand, Cybersecurity along with GenAI has several problems, such as adversarial AI threats, ethical concerns, and computational load. Making sure that AI generated threat intelligence is not biased, it is accurate, and it cannot be manipulated is a top priority for its weekly effective deployment. We would like to combat these cybersecurity challenges by putting forward a consolidated approach combining GenAI and quantum-resistant cryptography. The proposed Threat Intelligence Platform (TIP) will be used to provide resilience, fighting the current and future cyber threats [4][7].

3. Proposed System Architecture

Threat Intelligence Platform (TIP) architecture is what is specifically designed for overcoming the ability to face the multifaceted challenges of modern cybersecurity. Its construction is such that it is flexible and adaptable to the changing scenario and the ever-growing threats out there, thanks to a modular and a scalable framework that it is built on.

3.1 Data Ingestion Layer

The Data Ingestion Layer forms the core of the platform where it carries out the task of collecting, preprocessing, and preparing data for an analysis. The core activity of this layer is to make sure that the platform has data, which is the highest quality, structured, and contextualized.

3.1.1 Data Sources

- **Network Logs:** It houses the data that the firewalls, intrusion detection systems (IDS), and network traffic analysers capture. This may consist of metadata which may include IP addresses, ports (source/destination), protocols, and packet payloads.
- **Endpoint Devices:** This is made possible by pulling out telemetry data from user devices (for example laptops, mobile phones) and servers, this includes process activity, file changes, and login attempts.
- **External Threat Feeds:** The feature is global threat intelligence providers (e.g., AlienVault, Virus Total) that supply information on known malware, phishing campaigns, and vulnerabilities.
- **Cloud Services:** It examines cloud infrastructure (e.g., AWS CloudTrail, Azure Security censer) for misconfigurations, illegal entry, and unusual activity.
- **Application Logs:** The logs collected from enterprise applications, databases, and APIs are analysed to find out whether application-layer attacks such as SQL injection or cross-site scripting (XSS) are involved in any sensitized data breaches. Figure 1 shows Data Ingestion Workflow.

3.1.2 Preprocessing

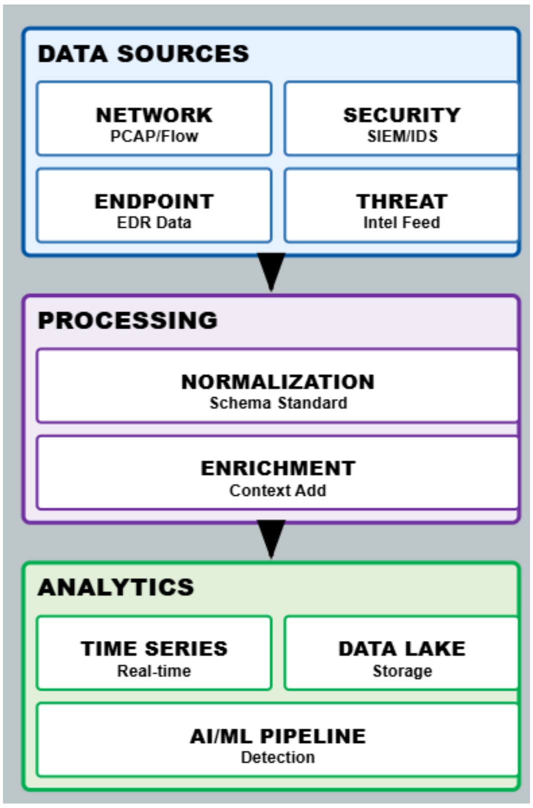

Figure 1 Data Ingestion Workflow

- **Normalization:** The process of converting JSON, XML, and Syslog into a single schema so that they can be analysed consistently.
- **Enrichment:** Metadata that is related to data e.g. location the data was taken (via IP addresses), threat severity scores and the stations in historical context (e.g. wherever the IP was flagged before) is added.
- **Filtering:** The procedure is taking the unnecessary and redundant data out of the original data, e.g. system update messages, which is thus clearing the noise and improving processing speed.
- **Data Deduplication:** A function where the software identifies duplicate entries by comparing them and deletes them to ensure only correct data is processed on the platform [5].

3.2 Generative AI Engine

The Generative AI Engine is the platform's intelligence center, which relies on sophisticated AI models to forecast, find, and react to threats in hot pursuit. Figure 2 shows Generative AI Engine Workflow.

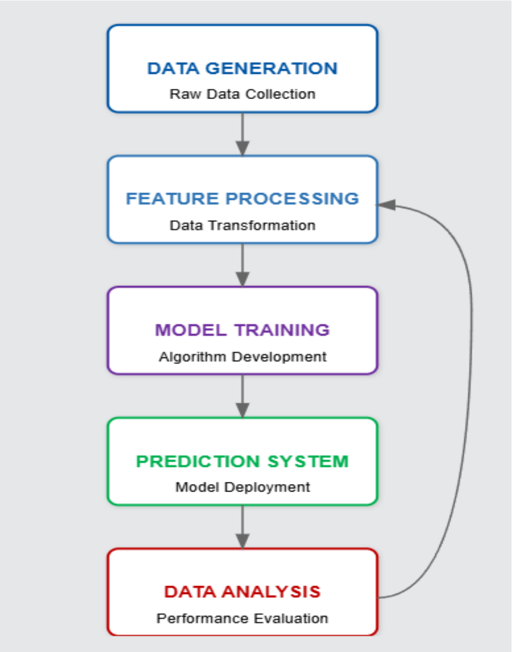

Figure 2 **Generative AI Engine Workflow**

- **Threat Scenario Modeling:** Simulation of Attack Vectors: This method uses Generative Adversarial Networks (GANs) to generate the most realistic attack scenarios. For instance, the AI may pretend to be a ransomware attacker against the corporation to find any possible flaws of the infrastructure.
- **Predictive Analytics:** Machine learning algorithms like Random Forest, Gradient Boosting), help in the recognition of the future by analyzing historical data and trends.
- **Synthetic Data Generation:** It is a method that is used to create synthetic datasets and train AI in recognizing the rare types of new patterns. A zero-day exploit that has no or little historical data to be detected is one of the cases that it can be most applicable with [8-10].

3.3 Quantum-Security Module

The Quantum-Security Module is an innovative cyber-attack prevention technology that is designed to guard both quantum and classical-based attacks on the platform by incorporating quantum resilient cryptographic algorithms. The security thrasher is featured with the functions, which makes it possible for the platform to fight off attackers, whether they are using common or quantum-style tactics.

3.3.1 Quantum-Resistant Algorithms

- **Lattice-Based Cryptography:** It has made robust security real by relying on the confusion of latte problems that are resistant to quantum noise A lattice happens to be the n-dimensional realization of a periodic structure. It is a fact that adding large amounts of quantum noise sends the phase of the latte structures to a point where they become random patterns.
- **Hash-Based Signatures:** By employing the technology of one-time signatures and Merkle trees, it gives a universal guarantee to the family of non-secure quantum-resistant digital signatures even if those were obtained here. The hash-based signature is typically produced via the one-time signature (OTS) scheme, which allows a one-time use type of signature. In addition to the OTS scheme, the hash tree-based cryptography is also used, which organizes keys in a binary tree. The family of those digital signatures that use quantum-resistant algorithms is globally secure, what means that you can trust a digital signature

not being compromised even if the platform where you obtained it is no secure. For a basic case, the universal hash function will be the one that you will pick to go with the one-time signature in the hash-based signature implementation. The private keys will no more be the deciding factor in the ownership of the public key, like they become when the traditional environmental systems like financial organizations[13-16].

3.4 Analytics and Visualization Layer

This area processes data to obtain actionable insights as well as comprehensive details of the threat landscape with advanced analytics and intuitive visualization tools.

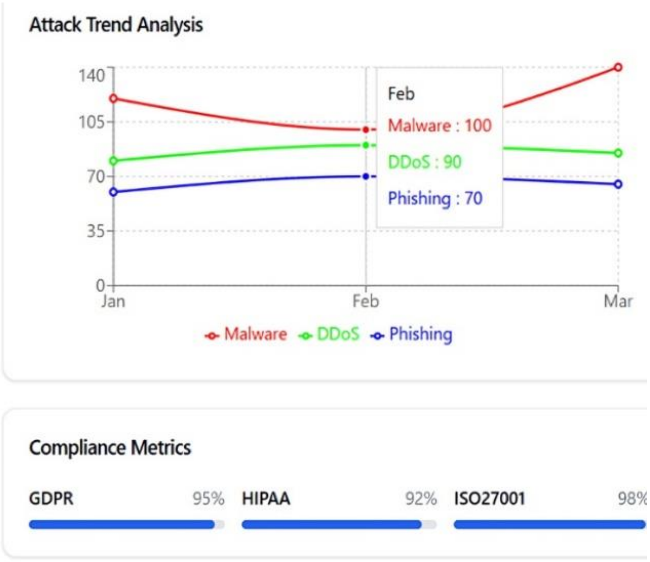

Figure 3 Visualization of the Attack Trend Analysis

4. Key Features and Innovations

The Threat Intelligence Platform proposed herein incorporates advanced technologies to enhance threat detection, response automation, and crypto resilience. This section describes the salient features and innovations distinguishing the platform from traditional cybersecurity solutions.

4.1 Predictive Threat Intel

Traditional threat intelligence systems have been reactive in nature, identifying threats only after an attack took place. In contrast, the proposed TIP uses Generative-AI (GenAI) to predict attack scenarios ahead of time.

- **Threat Scenario Modeling:** The system makes use of generative models such as Generative Adversarial Networks (GANs) and transformer-based architectures to realize possible cyberattack strategies. These models analyze historic attack data, contemporaneous threat intelligence feeds, adversary tactics to generate a realistic threat scenario.
- **Early Detection of Threat Indicators:** The system correlates threat-intelligence data drawn from various domains: for instance, network logs and endpoint telemetry from investigation of dark web. By following such proactive methodology, security teams can anticipate attack vectors even before they are weaponized.
- **Real-Time Risk Assessment:** Thus, in a continuous, real-time manner, the platform assesses the risk level resulting from any new threats based on a risk scoring mechanism. Using ML-driven anomaly detection in combination with probabilistic risk models, TIP alerts the organization on imminent threats and suggests countermeasures long before an incident escalates.

4.2 Adaptive Anomaly Detection

Traditional anomaly detection systems suffer from high false-positive rates and limited adaptability to evolving attack techniques. The TIP enhances detection accuracy by implementing an adaptive AI-driven anomaly detection framework that dynamically refines its threat identification capabilities.

- **Behavioural Analytics:** The TIP integrates User and Entity Behaviour Analytics (UEBA) to monitor deviations in user activities and system interactions. By analysing time-series data, access logs, and privilege escalation attempts, the platform identifies suspicious behaviours indicative of insider threats, credential misuse, or unauthorized access attempts.
- **Zero-Day Attack Detection:** Using adversarial AI techniques, the platform generates synthetic attack simulations to train its models for detecting zero-day exploits.

Conclusion

The recommended Threat Intelligence Platform integrates Generative Artificial Intelligence with quantum-resistant security to boost cyber-hygiene resilience. In so doing, it allows for predictive threat modelling, anomaly detection, and automated response, thereby fortifying the mechanisms of real-time defenses. With a post-quantum cryptographic algorithm employed in its backdrop, long-lasting protection with high assurance could be ensured for data against growing threats. Some of the hurdles in the way of this research include computational requirements and standardization; nevertheless, the work sets a stepping stone for future development in news. So, AI meets quantum security with a view toward protecting critical systems as we transverse an ever-shifting digital landscape. Thus, the pathway should be laid for upcoming intelligent and quantum-secure solutions as a route of safeguarding infrastructures against futuristically sophisticated cyber-attack threats.

References

[1]. Kumar, A., Singh, P., & Kumar, R. (2022). Modern SIEM: Current challenges and future directions. IEEE Transactions on Information Forensics and Security, 17, 2452-2467.

[2]. Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., & Tihanyi, N. (2024). Generative AI and Large Language Models for Cyber Security: All Insights You Need. arXiv preprint arXiv:2405.12750.

[3]. Fieblinger, R., Alam, M. T., & Rastogi, N. (2024). Actionable Cyber Threat Intelligence using Knowledge Graphs and Large Language Models. arXiv preprint arXiv:2407.02528.

[4]. Khurana, N., Mittal, S., Piplai, A., & Joshi, A. (2020). Preventing poisoning attacks on AI based threat intelligence systems. In IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 1021-1028).

[5]. Gopu, A., et al. (2023). Energy-efficient virtual machine placement in distributed cloud using NSGA-III algorithm. J. Cloud Comput., 12(1), 124.

[6]. Haryanto, C. Y., Elvira, A. M., Nguyen, T. D., Vu, M. H., Hartanto, Y., Lomempow, E., & Arakala, A. (2024). Contextualized AI for Cyber Defense: An Automated Survey Using LLMs. In Proc. 17th Int. Conf. Security of Information and Networks (SIN) (pp. 1-8).

[7]. Hasanov, I., Virtanen, S., Hakkala, A., & Isoaho, J. (2024). Application of Large Language Models in Cybersecurity: A Systematic Literature Review. IEEE Access, 12, 176751-176778.

[8]. [Radanliev, P., De Roure, D., & Santos, O. (2023). Red Teaming Generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved Quantum-Resistant Cryptographic Algorithms. arXiv preprint arXiv:2310.04425.

[9]. Sahay, S. K. (2023). AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. IEEE Access, 11, 123456-123470.

[10]. Vadisetty, R., & Polamarasetti, A. (2024). Generative AI for Cyber Threat Simulation and Defense. In Proc. 12th Int. Conf. Control, Mechatronics and Automation (ICCMA) (pp. 272-279).

[11]. Zhang, J., et al. (2024). Generative AI for Cyber Threat Simulation and Defense. In Proc. IEEE Symp. Security and Privacy (SP) (pp. 1-15).

[12]. [Park, T. H., Kim, J. K., & Lee, S. Y. (2023). Groq-driven acceleration for AI-powered cybersecurity applications. In IEEE International Conference on Artificial Intelligence and Cybersecurity (ICAIC) (pp. 213-220).

[13]. Abdel-Basset, M., Chang, V., & Hawash, H. (2023). Quantum-resistant cryptographic approaches for securing future cybersecurity infrastructures. Future Generation Computer Systems, 142, 248-263.

[14]. Walter, C., Henzler, P., & Lanzenberger, M. (2024). Visualizing cyber threat intelligence: A survey on visual analytics approaches. IEEE Transactions on Visualization and Computer Graphics, 30(3), 1532-1551.

[15]. Alvarez, M., Cheng, L., & Takahashi, H. (2024). Advanced Threat Intelligence

Platforms: A Comparative Analysis of AI-Empowered Detection Capabilities. IEEE Security & Privacy, 22(1), 32-47.

[16]. Kim, H. J., Barton, A., & Fernandez, E. (2023). Quantum-Resistant Authentication and Encryption Methods for Next-Generation Security Frameworks. IEEE Access, 11, 134982-135001.