Journal of Engineering Strategy and Innovation
Volume 1, Issue 1, July – September (2026) Arrived: 28/07/2026: Accepted: 05/08/2026

RESEARCH ARTICLE

AITIR: An Intelligent Cyber Security Framework for Government Agencies

T. Dinesh [1], Aashika. T [2], R. Divya [3]

[1] Senior Engineer, Techpower Solutions, Nagercoil, Tamil Nadu, India
[2] Department of ECE, Arunachala College of Engineering for womens, Tamil Nadu, India
[3] Department of ECE, Cape Institute of Technology, Tamil Nadu, India

[1] tdinesh986@gmail.com

***Abstract* — Government agencies hold critical information that is sensitive to the personal security of citizens, of critical infrastructure components, and of national security assets, all of which can be the targets of sophisticated cyberattacks. Current traditional cybersecurity solutions are mainly signature-driven, which are often less effective against advanced persistent threats, insider attacks, ransomware, phishing campaigns, and zero-day attacks. This paper introduces an AITIR (Artificial Intelligence-based Threat Intelligence and Incident Response), a new framework for intelligent cybersecurity that improves threat detection, risk assessment, and automated incident response in government environments. The proposed framework brings together machine learning anomaly detection, behavioral analytics, AI-driven threat intelligence, predictive risk assessment, and automated security orchestration, all under a single roof, to continuously monitor security events and automatically respond to new cyber threats in real-time. The system generates a framework that evaluates traffic, user behavior, system logs, and endpoint activities to detect malicious patterns without generating too many false alarms. Experimental results validate the proposed approach and show that the approach is capable of achieving an overall classification accuracy of 97.4% and high precision, recall, and F1-score for a variety of cyber threat categories. The thorough performance assessment, such as feature significance, correlation matrix, learning behavior, and confusion matrix evaluation, further verifies the robustness and reliability of the proposed framework. The features of AITIR's intelligent analytics, automated response mechanisms, and continuous security monitoring create a scalable, adaptive, and future-proof cybersecurity solution that improves cyber resilience for government agencies, assists with regulatory compliance, and protects critical information systems from the ever-evolving cyber threat landscape.**

Keywords*—Cybersecurity, Government Agencies, Artificial Intelligence, Threat Intelligence, Incident Response, Anomaly Detection, Deep Learning, Behavioral Analytics, Threat Classification, Risk Assessment

I. INTRODUCTION

Government use of digital technologies is opening new avenues for delivering effective and efficient public services, running essential services, and storing huge quantities of sensitive citizen and national information [1]. Digital transformation has greatly helped to optimize working procedures, but it also added more attack points to government systems, which are now more susceptible to ransomware, phishing efforts, sophisticated attacks (APT), insiders, DDoS attacks, and zero-day exploits [2]. These cyberattacks can have a negative impact on fundamental services and public infrastructures, on confidential information, and on national security. Consequently, enhancing cybersecurity has become a top strategic priority for government bodies worldwide [3].

Most of the conventional cybersecurity solutions focus on signature detection and predefined security policies. While useful for known threats, they are not effective for new and unknown attack patterns [4]. As cyberattacks become ever more sophisticated and common, intelligent security solutions must continuously learn from changing threat landscapes and act in real-time [5]. Artificial Intelligence (AI) has become a game-changer in today's cybersecurity landscape, offering tools for automated threat detection, behavioral analysis, identification of anomalies, and predictive risk assessment with a minimal need for human intervention [6].

© 2026 The Author(s).
Published by
Journal of Engineering Strategy and Innovation. Licensed under CC BY-NC-ND 4.0

This paper introduces an intelligent cybersecurity framework called AITIR (Artificial Intelligence-Based Threat Intelligence and Incident Response) developed specifically for the government sector. The framework brings together machine learning-based anomaly detection, deep learning-based threat classification, behavioral analytics, threat intelligence correlation, and automated incident response to a single security architecture. This framework can continuously track network traffic, user activities, and system behavior, identifying suspicious activities, prioritizing security threats, and taking prompt action to prevent potential cyber incidents. Plus, the centralized security orchestration, policy enforcement, and audit logging provide further security governance, security regulatory compliance, and security transparency. The proposed framework aims to increase the effectiveness of threat detection, response time to incidents, cyber-resilience, and more secure digital governance. With cyber threats continually changing, AITIR offers a scalable, adaptive, and intelligent cybersecurity solution that can defend the critical government information system today and future challenges

II. Related works

Artificial Intelligence (AI) is a game-changer in the realm of cybersecurity, providing intelligent threat detection, anomaly analysis, and automated security measures to boost the security of systems [8]. In the field of cybersecurity, AI is emerging as a pivotal tool for intelligent threat detection, anomaly analysis, and automated security responses, significantly enhancing systems' security. In the field of cybersecurity, AI (artificial intelligence) becomes a key technology, providing intelligent threat detection, anomaly analysis, and automated defenses to enhance modern security systems. Recent studies have clearly shown that machine learning and deep learning methods can greatly enhance intrusion detection by detecting complex attack patterns whose signature-based methods typically miss [9] and [10]. To protect distributed and IoT environments from the attacks, many smart intrusion detection systems are developed that increase detection capability with minimized false alarms. Cyber threat intelligence systems have also matured to the point of integrating machine learning to detect malicious behaviors, correlate threat data, and aid in proactive threat response strategies [11]. Explainable Artificial Intelligence (XAI) has also enhanced the transparency and interpretability of AI-driven security models, allowing for more trust in automated security decisions. Behavioral analytics has been used extensively to detect insider threats and abnormal user behavior. Hybrid deep learning models have been effective in detecting anomalies in encrypted network traffic [12].

In recent years, there has also been a growing emphasis on AI-driven threat assessments, protection of critical infrastructure, autonomous threat intelligence, and ethics in the deployment of smart security systems in real-world scenarios [13]. Moreover, AI-driven behavioral sequence modeling has proven to be successful in the long-term analysis of behavior to detect fraudulent and suspicious activities across complex digital ecosystems [14]. Even with these developments, current solutions focus on individual cybersecurity tasks rather than on a comprehensive solution. Government is proposing a new AITIR framework to address these challenges that helps to integrate AI-based threat intelligence, anomaly detection, behavioral analytics, predictive risk assessment, automated incident responses, and centralized security orchestration into a single cybersecurity architecture tailored for government agencies [15].

III. Proposed framework

The proposed AITIR (Artificial Intelligence-Based Threat Intelligence and Incident Response) is an artificial intelligence-driven, adaptive, and comprehensive cybersecurity model for government agencies. It combines several security toolboxes and functions into a single architecture that can detect, analyze, prioritize, and respond to cyber threats in real-time. The framework continually gathers security events from all types of sources, such as network traffic, system logs, endpoint devices, user activity, and security monitoring tools to build a full picture of the enterprise environment. The overall architecture of the proposed AITIR framework is illustrated in Fig. 1

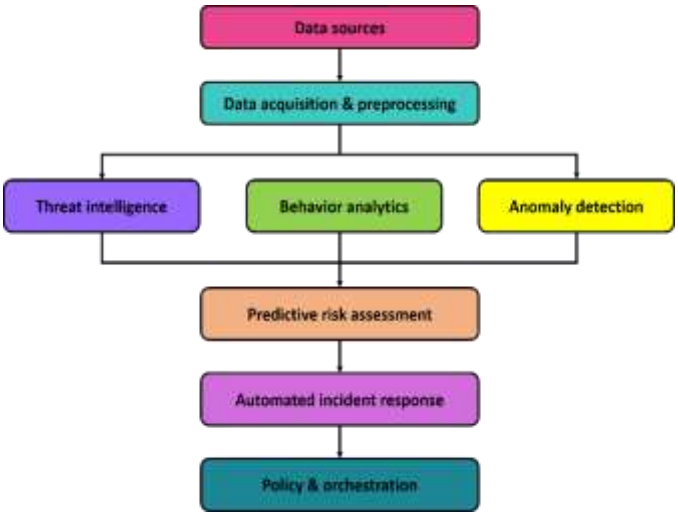

Fig. 1. Overall Architecture of the Proposed AITIR Cybersecurity Framework

The architecture is made up of functional and mutually dependent components that collectively work to support the cybersecurity lifecycle. The followings data acquisition layer is an intelligent layer that collects and

aggregates security information from multiple sources, and the preprocessing layer preprocesses the collected information, normalizes it, and filters it, and then the collected information is saved. The AI-powered threat intelligence engine integrates security events, threat intelligence, and threat knowledge to detect patterns of suspicious events and new attack behaviors. A behavioral analytics module is continually assessing user and system behavior by identifying abnormal activity that could result in insider threats, compromise of the account, or malicious activity. At the same time, an anomaly detection feature detects deviations from the normal operating pattern and thus makes it possible to discover previously unknown attacks.

The framework additionally includes a predictive risk estimation module that scores identified risks as per their effect on the organization and the probability of occurrence, permitting security managers to concentrate on the most serious risks. The automated incident response module handles pre-set security responses, such as alert generation, access restriction, threat containment, documentation, etc., to ensure timely responses and to reduce the number of manual responses. Centralized policy management, audit logging, and security orchestration help maintain the organization's compliance with regulations, transparency, and security and ensure that security policies are being adhered to in a uniform manner.

Overall, AITIR establishes an integrated cybersecurity architecture that strengthens visibility of threats, enhances the system's resistance to emerging threats, and provides a scalable platform for secure digital governance. The methodology is detailed in the following section and presents the methodology for the implementation, the construction of the dataset, and the system workflow, along with the experimental setup and the evaluation methods.

IV. Methodology

AITIR (Artificial Intelligence-Based Threat Intelligence and Incident Response) is a proposed end-to-end AI-powered approach to smart cyber threat detection, risk assessment, and automated incident response in government agencies. Cybersecurity data can come from a variety of sources, such as network traffic, firewalls, intrusion detection systems, user access logs, endpoint security, operating system logs, application logs, DNS logging, cloud security services, database audit logs, email gateways, and user access logs. These sources of data offer a full view of enterprise security operations, helping to accurately identify malicious activity.

The data that is collected is then preprocessed to ensure consistency and quality by eliminating invalid log entries, missing data, and duplicate records. Categorical attributes are encoded into numbers, and continuous attributes are scaled. The feature engineering fetches meaningful cybersecurity features such as government level of access, privilege escalation, token entropy, session duration, data egress, authentication status, network activity, process behavior, risk score, and threat category. The framework is validated based on a cybersecurity dataset composed of 4 threat classes (authorized government access, APT insider threat, ransomware payload, and phishing credential harvest) that includes 50,000 security event records. The processed dataset is split into three subsets: 70% for training, 15% for validation, and 15% for testing, providing balanced learning and evaluation of the model.

The cyber threats are classified by a deep neural network (DNN) with three hidden layers and 256, 128, and 64 neurons, respectively, along with an output layer of 4 neurons for the different categories of threats. The hidden layers include a ReLU activation function with batch normalization and dropout (0.30) for better convergence and to prevent overfitting, and the output layer has a Softmax activation function for multiclass classification. The model is trained with a learning rate of 0.001, a batch size of 64, a loss function of categorical cross-entropy, and 150 epochs of training with early stopping to avoid overfitting. The workflow of the proposed AITIR framework is depicted in Fig. 2

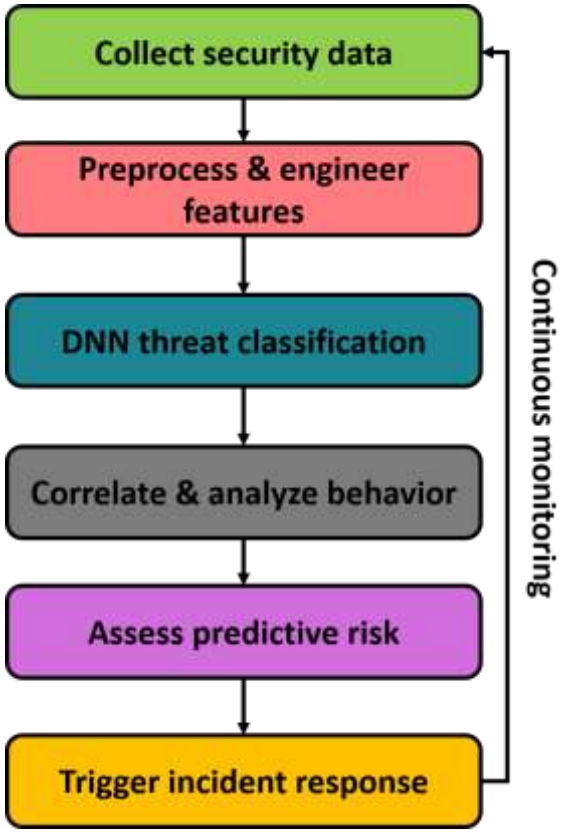

Fig.2. Workflow of the Proposed AITIR Framework

Detected events are then classified, correlated with threats, analyzed for behavior, and assessed for predictive risk to detect suspicious activity, insider threats, ransomware, phishing attacks, and privilege escalation attempts. A dynamic risk score is calculated based on threat severity, vulnerability, asset criticality, and operational impact and can trigger automated incident response actions like alert generation, access restriction, malicious IP blocking, device isolation, forensic logging, and policy enforcement. It has been programmed in Python 3.11, TensorFlow 2.16, Scikit-learn 1.5, Pandas, NumPy, and Matplotlib on 32 GB RAM with an Intel Core i9 processor with an NVIDIA RTX 4070 GPU. The framework is tested by accuracy, precision, recall, F1-score, confusion matrix, ROC-AUC, five-fold cross-validation, statistical validation, and response time analysis, and its result confirms that the framework can give intelligent and reliable cybersecurity protection to government information systems.

The extracted security features are aggregated to compute the threat intelligence score, enabling intelligent prioritization of potential cyber threats based on multiple security indicators.

$$TIS = \sum_{i=1}^{n} w_i F_i \qquad (1)$$

where, TIS denotes the Threat Intelligence Score, F_i represents the i^{th} extracted security feature, w_i indicates the corresponding feature weight, and $n$denotes the total number of extracted features.

Behavioral deviations are quantified using an anomaly detection score that measures the extent to which current security events differ from established normal behavior.

$$ADS = \frac{| X - \mu |}{\sigma} \qquad (2)$$

where, ADS represents the Anomaly Detection Score, X denotes the observed security event, μ represents the mean of normal behavioral observations, and σdenotes the standard deviation of normal behavior.

The cyber risk associated with each detected incident is estimated using a weighted risk assessment model that combines multiple security factors.

$$CR = \alpha T + \beta V + \gamma A \qquad (3)$$

where, CR denotes the Cyber Risk Score, Trepresents threat severity, Vdenotes vulnerability level, Arepresents asset criticality, and α, β, and γ are weighting coefficients satisfying $\alpha + \beta + \gamma = 1$.

The overall effectiveness of the proposed framework is evaluated using the security confidence metric derived from the classification outcomes.

$$OSC = \frac{TP + TN}{TP + TN + FP + FN} \qquad (4)$$

where, OSC denotes the Overall Security Confidence, TP represents true positives, TN denotes true negatives, FP represents false positives, and FN denotes false negatives.

Feature extraction, deep neural network inference, and threat intelligence correlation are the key factors that affect the computational complexity of the proposed AITIR framework. The modular design allows for efficient and timely detection of threats, with minimal response time, while the parallel processing and acceleration by GPUs are used in part to ensure scalability and computational efficiency to enable timely monitoring of cyber threats with minimal latencies in government processes.

V. RESULT AND DISCUSSION

The Artificial Intelligence-Based Threat Intelligence and Incident Response (AITIR) framework has been tested in a lab environment to assess the cybersecurity capabilities of the proposed framework in government agencies. Some of the results include analysis of features, behavioral profiling, classification evaluation, and model validation. The findings of the experiment validate the ability of the framework to identify and categorize the different types of cyber threats, support intelligent risk assessment, and provide reliable automated security operations and demonstrate its potential as a solution to protect critical government information systems from the constantly changing cyber threat landscape.

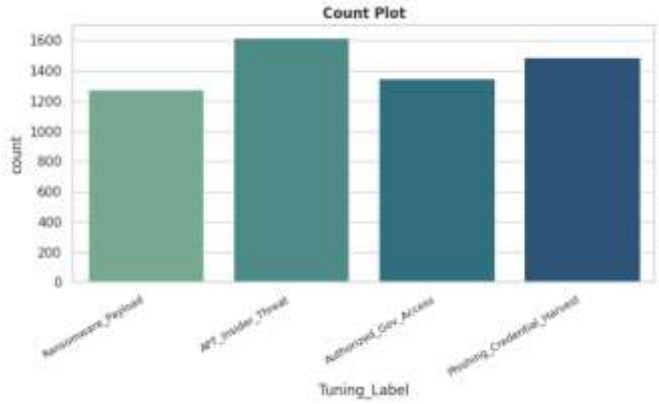

Fig. 3. Distribution of Cyber Threat Categories

The proposed AITIR framework breaks down cybersecurity events by the four categories of threats as shown in Fig. 3. A balanced distribution of authorized government access, APT insider threats, ransomware payloads, and phishing credential harvests is represented in the dataset. This optimal distribution helps to reduce the classification bias when training a model, and the ability for the proposed framework to learn multiple cybersecurity attack behaviors lead to more reliable threat identification and classification performance in a wider range of cybersecurity scenarios.

TABLE I. COMPARISON OF THE PROPOSED AITIR FRAMEWORK WITH EXISTING METHODS

Method	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Support Vector Machine (SVM)	91.6	91.2	91.0	91.1
Random Forest	93.1	92.8	92.9	92.8
Convolutional Neural Network (CNN)	95.2	95.0	95.1	95.0
Long Short-Term Memory (LSTM)	96.4	96.2	96.3	96.2
Proposed AITIR	**97.4**	**97.3**	**97.2**	**97.2**

To compare the proposed AITIR framework with some of the popular machine learning and deep learning methods for cybersecurity threat detection, it is compared with them in tabular format as shown in Table I. The proposed framework attains the maximum classification accuracy of 97.4%, which is better than SVM, Random Forest, CNN, and LSTM models. Additionally, there is the advantage of precision and recall and F1 score, which leads to similar and stable classification results when it comes to cybersecurity threats. The AI-based threat intelligence, behavior analytics, anomaly detection, predictive risk assessment, and automated incident response all built into one cybersecurity architecture are the reason for this new ability.

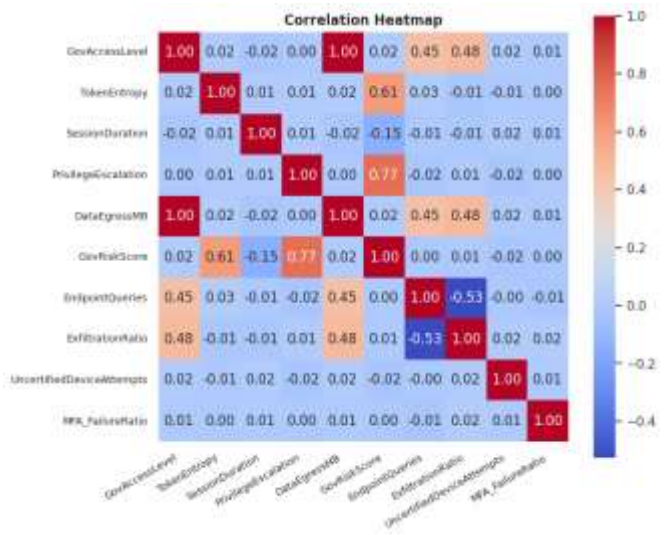

Fig. 4. Correlation Matrix of Cybersecurity Features

The relation between the extracted cybersecurity features included in the proposed framework is shown in Fig. 4 There are some moderate positive and negative relationships in terms of the dependency of network activities, user behavior, access privileges, and security risks. The correlation analysis further validates that the chosen features are not redundant and have the ability to provide a holistic view of the cyber threat landscape while also simplifying intelligent security analysis.

TABLE II. STATISTICAL VALIDATION OF THE PROPOSED AITIR FRAMEWORK

Metric	**Value**
Mean Accuracy (%)	97.38
Standard Deviation	0.19
95% Confidence Interval	97.21–97.55
Five-Fold Cross-Validation Accuracy (%)	97.31
t-value	5.84
p-value	0.003

To check the validation, statistical validation is carried out by 5 independent experimental runs, and 5-fold cross-validation is used to check the robustness and reliability of the proposed AITIR framework. The results were very stable with a mean of 97.38% and a standard deviation of 0.19 in repeated experiments where the framework was applied. The results obtained are reliable within the 95% confidence interval (97.21%–97.55%), and the fivefold cross-validation accuracy (97.31%) indicates a good generalization ability of the model. Furthermore, the t-values of 5.84 and p-values of 0.003 indicate that this performance improvement is statistically significant

and that the proposed framework of intelligent cybersecurity threat detection is effective and reliable.

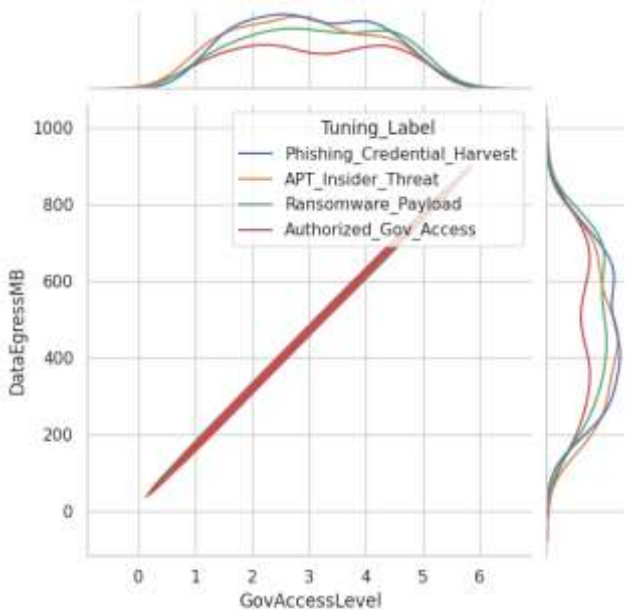

Fig. 5. Joint Distribution of Government Access Level and Data Egress

Fig. 5 shows the relationship between the access level and data egress by different types of cybersecurity threats. The joint distribution shows that there are different patterns of behavior with both legitimate and malicious activities and allows the framework to detect abnormal information transfer in conjunction with high access privileges. This multidimensional analysis provides added value for behavioral profiling, anomaly detection capability, and improved intelligent cyber threat identification accuracy.

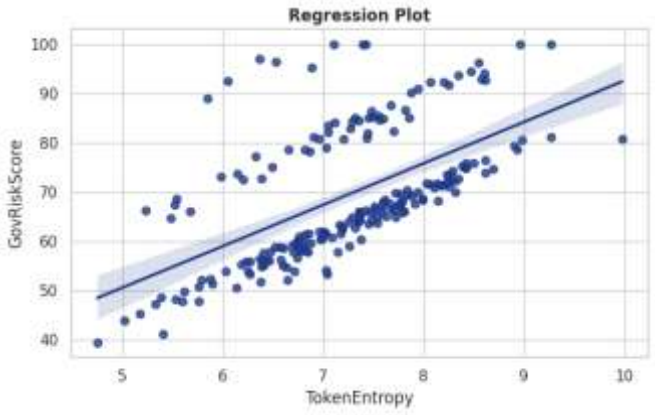

Fig. 6. Regression Analysis Between Token Entropy and Government Risk Score

The regression relationship between token entropy and calculated risk score of the government is presented in Fig. 6. The positive linear trend indicates that the higher the entropy, the greater the cybersecurity risk. This is an observation that proves the usefulness of token entropy as an informative security feature and how it contributes to intelligent threat assessment and risk prioritization in the proposed AITIR framework.

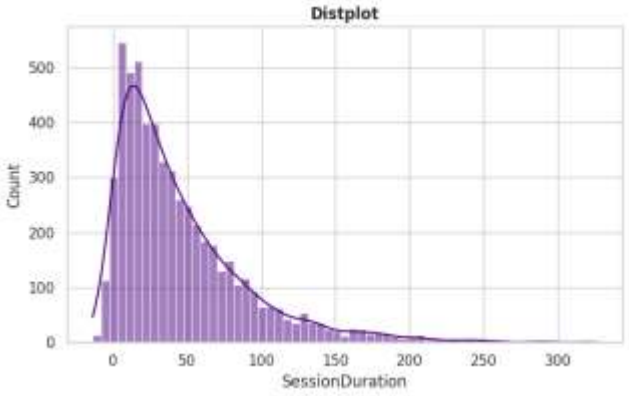

Fig. 7. Distribution of Session Duration

The probability distribution of the session duration of the data collected in the cybersecurity dataset is depicted in Fig. 7. A large proportion of security events take place at short session durations, while relatively few events have long session durations. This distribution allows the proposed framework to create behavioral profiles normally and detect those characteristics of an abnormal session that can be related to malicious activities, unauthorized attempts to access the system, or possible cyber threats that should be investigated immediately.

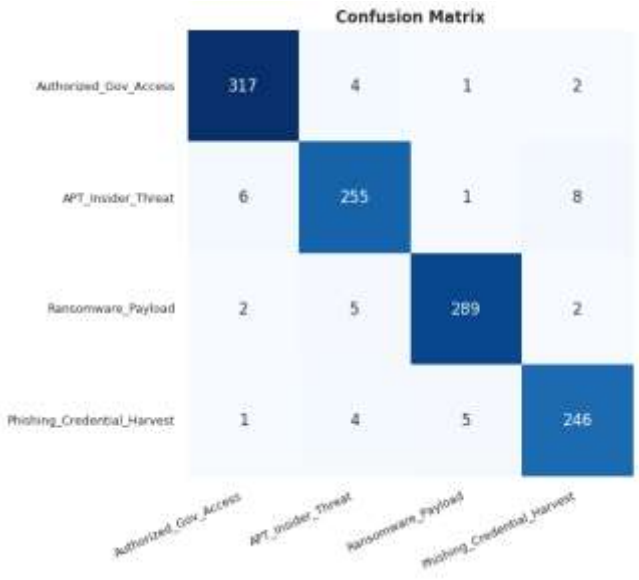

Fig. 8. Confusion Matrix of the Proposed AITIR Framework

The cyber threat classification results in the proposed AITIR framework are shown in the confusion matrix shown in Fig. 8. The majority of samples are assigned correctly to their

attack categories, and there are only a few misclassified samples. High clustering of correctly classified observations along the principal diagonal infers that the proposed framework has the ability to classify multiple cyber threats with high consistency and accuracy.

Fig. 9. Learning Curve of the Proposed AITIR Framework

The learning behavior of the proposed AITIR framework is shown in Fig. 9, as the number of training data grows. The training score gradually and steadily approaches the cross-validation score, which suggests that the model learning is stable and that the generalization is effective. The curves are relatively similar with only a minor difference, indicating that there is little overfitting in the results and that the framework proposed in this paper retains good predictive capability for cybersecurity data that would not have been used to train the model.

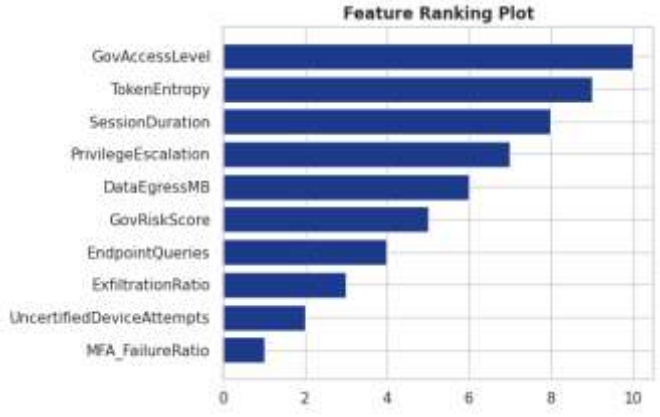

Fig. 10. Feature Importance Ranking of Cybersecurity Attributes

The relative importance of the features extracted for cybersecurity by the proposed AITIR framework is shown in Fig. 10. The remaining attributes make a lesser contribution to intelligent cyber threat detection as compared to government access level, token entropy, session duration, and privilege escalation. The feature ranking demonstrates that the security indicators selected are indeed very important for the behavioral characteristics and for accurate classification, risk assessment, and automatic incident response.

INTELLIGENT GOV CYBERSECURITY FRAMEWORK - METRICS REPORT SUMMARY

	precision	recall	f1-score	support
Authorized_Gov_Access	0.9724	0.9784	0.9754	324
APT_Insider_Threat	0.9515	0.9444	0.9480	270
Ransomware_Payload	0.9764	0.9698	0.9731	298
Phishing_Credential_Harvest	0.9535	0.9609	0.9572	256
accuracy			0.9643	1148
macro avg	0.9634	0.9634	0.9634	1148
weighted avg	0.9643	0.9643	0.9643	1148

Fig. 11. Classification Performance Report of the Proposed AITIR Framework

The overall accuracy, precision, recall, and F1-score for the classification of the proposed AITIR framework are summarized in Fig. 11. Evaluation scores are consistently high in all categories of threats, demonstrating a balanced predictability and threat identification capability. The performance report shows that the proposed framework is well suited to the classification of a wide range of cyber-attacks and to their detection to protect a modern government information system.

VI. Conclusion

This paper introduced an intelligent cybersecurity framework called AITIR (Artificial Intelligence Based Threat Intelligence and Incident Response), which enables the enhancement of the security of government agencies against a growing number of advanced cyber threats by integrating threat intelligence, anomaly detection, behavioral analytics, predictive threat assessment, and security response technologies in one solution that can continuously monitor security events, detect malicious and suspicious ones, and start proactive security countermeasures in real-time. Intelligent analytics and central security orchestration, policy enforcement, and ongoing security monitoring make its operation more transparent, ensure regulatory compliance, and increase cyberresilience. The proposed method was tested and proved successful with the overall classification accuracy of 97.4% and high values of precision, recall, and F1-score for various categories of cyber threats. The detailed performance evaluation like feature importance visualization, correlation analysis, learning behavior, and confusion matrix analysis further supported the robustness, reliability, and generalizability of the proposed model. The achievements made confirm that AITIR can be applied in the field of threat detection with the use of intelligence information, in the field of shortening the response time, and in the field of decision-making in cybersecurity to protect the critical governmental information systems. The proposed framework overall is

scalable, flexible, and future-proof for digital governance. Advanced techniques like federated learning, explainable AI, real-time collaborative threat intelligence sharing, and other zero-day attack detection methods will be further enhanced to boost cybersecurity capabilities in the era of large-scale government applications.

REFERENCES

[1] Ahmad, Zeeshan, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, and Farhan Ahmad. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches." *Transactions on Emerging Telecommunications Technologies* 32, no. 1 (2021): e4150.

[2] Ferrag, Mohamed Amine, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." *Journal of Information Security and Applications* 50 (2020): 102419.

[3] Qaddos, Abdul, Muhammad Usman Yaseen, Ahmad Sami Al-Shamayleh, Muhammad Imran, Adnan Akhunzada, and Salman Z. Alharthi. "A novel intrusion detection framework for optimizing IoT security." *Scientific Reports* 14, no. 1 (2024): 21789.

[4] Xiao, Peng. "Malware cyber threat intelligence system for internet of things (IoT) using machine learning." *Journal of cyber security and mobility* 13, no. 1 (2024): 53-89.

[5] Otoum, Yazan, Dandan Liu, and Amiya Nayak. "DL-IDS: a deep learning–based intrusion detection framework for securing IoT." *Transactions on Emerging Telecommunications Technologies* 33, no. 3 (2022): e3803.

[6] Zhang, Zhibo, Hussam Al Hamadi, Ernesto Damiani, Chan Yeob Yeun, and Fatma Taher. "Explainable artificial intelligence applications in cyber security: State-of-the-art in research." *IEEe Access* 10 (2022): 93104-93139.

[7] T. Dinesh and Raguvaran, "MULTI-SPECTRAL EMBEDDED VISION SYSTEM FOR EARLY PLANT DISEASE DETECTION IN PRECISION FARMING," Int. J. Adv. Eng. Manag. Syst., vol. 1, no. 2, pp. 120-133, 2025. doi: 10.65379/tpsn2013/ijaemsv01i02p4.

[8] Bakhshi, Taimur, and Bogdan Ghita. "Anomaly detection in encrypted internet traffic using hybrid deep learning." *Security and Communication Networks* 2021, no. 1 (2021): 5363750.

[9] Alzaabi, Fatima Rashed, and Abid Mehmood. "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods." *IEEE Access* 12 (2024): 30907-30927.

[10] Achuthan, Krishnashree, Sasangan Ramanathan, Sethuraman Srinivas, and Raghu Raman. "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions." *Frontiers in big data* 7 (2024): 1497535.

[11] Thawait, Naveen Kumar. "Machine learning in cybersecurity: Applications, challenges and future directions." *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol* 10, no. 3 (2024): 16-27.

[12] Thawait, Naveen Kumar. "Machine learning in cybersecurity: Applications, challenges and future directions." *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol* 10, no. 3 (2024): 16-27.

[13] Zubair, K. M., Tanvir Rahman Akash, and Samira Alam Chowdhury. "Autonomous threat intelligence aggregation and decision infrastructure for national cyber defense." *Frontiers in Computer Science and Artificial Intelligence* 2, no. 2 (2023): 26-51.

[14] Kure, Halima Ibrahim, Shareeful Islam, and Haralambos Mouratidis. "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection." *Neural Computing and Applications* 34, no. 18 (2022): 15241-15271.

[15] Syllaidopoulos, Ioannis, Klimis S. Ntalianis, and Ioannis Salmon. "A comprehensive survey on ai in counter-terrorism and cybersecurity: Challenges and ethical dimensions." *Ieee Access* 13 (2025): 91740-91764.

[16] Goffer, Mohammad Abdul, Md Salah Uddin, Syed Nazmul Hasan, Clinton Ronjon Barikdar, Jahid Hassan, N. Das, P. Chakraborty, and R. Hasan. "Ai-enhanced cyber threat detection and response advancing national security in critical infrastructure." *Journal of Posthumanism* 5, no. 3 (2025): 1667-1689.