Milestone Transactions on
Artificial Intelligence
Vol. 01 | Issue. 01 | 2026

RESEARCH ARTICLE OPEN ACCESS

AI-Driven Approaches for Developing Effective Cybersecurity Policies and Procedures

P Bhanu Prakash[*]. S Siva Sankar . P Sudarshan . G Mohan Krishna . V Revanth Sai

Department of CSE (IoT, Cyber Security including Block Chain Technology),
Annamacharya Institute of Technology & Sciences (Autonomous),
Tirupati, Andra Pradesh, India.

DOI: **10.5281/zenodo.18525711**
Received: 21 January 2026 / Revised: 28 January 2026 / Accepted: 7 February 2026

**Corresponding Author: bhanuprakash.p1311@gmail.com*

Abstract – The increasing complexity of cyber threats, coupled with the rapidly increasing pace of digital transformation fueled by cloud computing, IoT, and interconnected enterprise systems, has exposed the limitations of traditional, static cybersecurity policies and procedures. Traditional approaches are largely manual and compliance-oriented, and are not dynamic enough to keep up with the ever-changing nature of cyber threats such as zero-day attacks, advanced persistent threats, and AI-powered social engineering. Our objectives are to design an AI framework for automated generation of cybersecurity policies and procedures, enabling intelligent, data-driven, and dynamic policy design. The proposed system employs Natural Language Processing (NLP) for policy knowledge extraction and a Support Vector Machine (SVM) classifier for policy component classification and validation based on relevance, compliance level, and organizational context. The system design has four layers: input and knowledge acquisition, feature engineering, AI-based decision modeling, and automated policy generation with version control. The experimental results on the NSL-KDD dataset demonstrated that the SVM classifier outperforms Logistic Regression, XGBoost, and Random Forest in terms of accuracy, achieving 99-100%, validating the effectiveness of the proposed system in detecting threat patterns that can serve as a basis for policy formulation. The analysis using the confusion matrix and ROC curve shows that the model is stable, with low false-negative rates, which is significant for proactive cybersecurity governance. The research also considers governance, ethics, and compliance by aligning AI-based policy mechanisms with existing standards such as NIST CSF and ISO. The findings show that AI can play an important role in making policies more responsive, reducing human error, improving compliance, and making policies evolve.

Index Terms – Artificial Intelligence, Cybersecurity Policy, Machine Learning, Support Vector Machine, Policy Automation, Threat Detection, Governance Frameworks.

I. INTRODUCTION

The rapid digitalization of modern organizations, facilitated by cloud computing, IoT, big data, and interconnected enterprise systems, has dramatically transformed the cybersecurity landscape. While digitalization has opened doors to greater efficiency, scalability, and innovation, it has also created a larger attack surface that exposes modern organizations to ever-evolving cyber attacks like APTs, zero-day attacks, ransomware attacks, insider attacks, AI-based social engineering attacks, etc. Conventional cybersecurity policies and procedures, which are often static, compliance-based, reactive, and change-averse, are no longer effective enough to combat these ever-evolving cyber attacks [1]. In this regard, there has been a significant need to employ intelligent, adaptive, and data-driven cybersecurity governance models that incorporate AI as a key component [2].

The role of AI and Machine Learning (ML) in cybersecurity is transforming the traditional cybersecurity environment from a rule-based defense system to a more intelligent, predictive, and autonomous system. AI systems have the potential to process large amounts of security log data, network traffic data, and user behavior patterns to detect unusual patterns, predict future attacks, and respond to them in real time [3]. The role of AI in the formulation of policies and procedures is not limited to the formulation of defense mechanisms; rather, it extends to strategic decision-making. For instance, generative AI systems have the potential to simulate various cyber attacks, analyze the effectiveness of existing defense systems, and provide recommendations for the modification of policies based on the identification of vulnerabilities [4]. This allows the organization to transform the traditional periodic evolution of policies to continuous evolution, ensuring the alignment of cybersecurity procedures with the ever-evolving cybersecurity environment [5].

Another notable advantage that AI offers with regard to cybersecurity governance stems from its capacity for automation and optimization. This feature, for instance, enables AI tools to automatically assess an entity's compliance with security standards, identify discrepancies from set procedures, and notify appropriate personnel. This helps eliminate human error, ensures consistency in policy execution, and boosts efficiency. Another notable aspect that AI offers with regard to security policy formulation stems from its capacity for risk-based policy formulation, where it combines threat intelligence, asset criticality, and vulnerability data. This aspect is vital, especially for larger entities where manual monitoring and policy execution would be impossible. However, the integration of AI in cybersecurity policy frameworks also poses complex governance issues. The use of autonomous decision-making systems poses legal, ethical, and accountability questions, particularly if the AI-driven actions impact critical infrastructure or user data [6]. The questions of bias, transparency, explainability, and trust need to be answered to ensure that AI-driven policies are fair, trustworthy, and compliant with regulatory requirements. Scholars have pointed out the need for governance frameworks that integrate AI innovation with legal, ethical, and human oversight [7]. In this context, the need to standardize AI-driven cybersecurity processes through frameworks such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and risk governance frameworks is imperative to ensure interoperability and standardization [8], [9].

Although tremendous progress has been made in the application of AI in threat detection and incident response, very little research has been conducted to specifically explore the role of AI in systematically supporting the development, improvement, and governance of cybersecurity policies and procedures. Most of the existing research has been based on technical aspects, and the organizational, procedural, and policy-based aspects have not been thoroughly investigated. To fill this research void, this study aims to explore the role of AI in designing adaptive cybersecurity policies, procedural updates, and strategic decision-making through data analytics and intelligent modeling. This study intends to offer a holistic view of how AI can improve cybersecurity resilience, response time, compliance, and organizational preparedness against cyber threats [10].

Our contributions are as follows:

- AI-Driven Cybersecurity Policy Engineering Framework: We propose a new framework that redefines the conventional cybersecurity policy engineering process from a manual, document-based approach to an intelligent, data-driven, automated process, where AI can support governance-level decision-making, rather than being limited to threat detection.
- SVM-Based Policy Relevance and Compliance Classification: We suggest a decision model that formalizes cybersecurity policy engineering as a classification problem. This model classifies policy statements by relevance and compliance strength, providing a mathematically grounded, evidence-based approach to selecting cybersecurity policies.
- NLP-Enabled Knowledge Extraction from Security Standards: We suggest that the proposed system could incorporate NLP-based feature representations of unstructured cybersecurity policies, security regulatory frameworks (e.g., NIST, ISO), and threat intelligence, enabling AI systems to learn governance knowledge from textual data.
- End-to-End Automated Policy Generation and Evolution Mechanism: We propose a comprehensive automated cybersecurity policy generation and evolution mechanism that encompasses the entire process of knowledge acquisition, feature engineering, AI-based decision modeling, automated policy generation, and evolution difference analysis.
- Data-Driven Link Between Intrusion Detection and Policy Formation: The paper, for the first time, introduces a link between AI-based intrusion detection performance metrics and the development of cybersecurity policies. This link helps form adaptive policies based on evidence rather than compliance.

II. LITERATURE SURVEY

The fast adoption of artificial intelligence (AI) in cybersecurity has redefined the manner in which organizations identify threats, manage risks, and formulate security policies. Nevertheless, recent developments in rapid AI adoption have also brought about new challenges in the areas of governance, compliance, and resilience, particularly in the case of generative AI. Radanliev et al. [1] presented a lifecycle-based generative AI governance framework based on the cybersecurity resilience and normative governance models. According to their research, there is a very large gap between fast AI integration and weak institutional protection, which results in new threats like shadow AI. The uniqueness of this piece is that it is a novel attempt to include ethics, security, and governance in an overall evaluative system. Nevertheless, the research has weaknesses associated with the use of secondary sources and a lack of empirical confirmation, which implies that practical and adaptive mechanisms of policy-generation are required.

Li et al. [2] investigated the intersection of big language models and cybersecurity with an interdisciplinary framework that uses agentic LLMs to analyze software security, network security, and vulnerability. Their design illustrates better automation and reason-based analytics by having a human-in-the-loop design. The study notes that although innovative, it faces critical challenges of limited interpretability, hallucinations, safety and fairness issues and lack of scalability to real-world applications, whereby strong governance and policy controls are necessary. A review of AI and machine learning methods in cybersecurity settings was made by Mohamed [3], covering such methods as deep learning-based intrusion detection, malware classification, behavioral anomaly detection, and intelligent threat analysis. The results suggest excellent results with comparison to conventional systems, especially with the zero-day and advanced persistent threats. However, the research unveils shortcomings of the high computational cost, the unintelligible nature, the problem of scalability, and the unavailability of standard benchmarks that restrict the functional deployment of such AI-based systems without policy frameworks.

McIntosh et al. [4] compared the key cybersecurity and governance frameworks available, such as NIST CSF 2.0, COBIT 2019, ISO/IEC 27001:2022, and ISO/IEC 42001:2023, to the adoption of LLC. With the help of a human-expert-in-the-loop evaluation model, the analysis identified the best model to support LLC opportunities in ISO/IEC 42001:2023, and the most appropriate to the EU AI Act was found in COBIT 2019. Nevertheless, the frameworks all have a lapse in the risk governance of LLM. The dependency of the qualitative method and the absence of the practical application point to the obvious gap in research on automated and adaptive policy enforcement. Gupta et al. [5] came up with a CNN-based security architecture of large language models, which are highly accurate on the KDDCup data set. The research synthesizes the analysis of global security landscapes with deep learning techniques, which are empirical in nature and overcome gaps in the validation of LLM security. However, it is restricted to using the outdated dataset and cannot apply to the current, real-life setting of an LLM-centric cyberattack that highlights the importance of updated datasets and policy-conscious assessment.

Casamassa et al. [6] proposed a coherent system of generative AI governance based on NIST AI RMF, COBIT 2019, and NIST CSF 2.0, to address the GAI-enabled cybersecurity risks. The research is valuable in that it aligns AI-specific risk management to enterprise IT governance and cybersecurity practices. Nevertheless, the structure is abstract and does not undergo any empirical experiments, which restricts its flexibility in high-paced generative AI conditions. In Kulothungan [7], the author explored ethical and regulatory requirements of AI-enhanced cybersecurity in terms of a conceptual risk-based and ethical framework. This analysis shows that there are irregular and partial international rules, which demonstrate the lack of a unified AI-cybersecurity regulation. Although, the study contributes to the policy and ethics discussion, its qualitative character and absence of empirical evidence restrain its feasibility.

Adapala and Alugubelly [8] introduced the Aegis Protocol, a layered security architecture of autonomous AI agents, which combines decentralized identity, post-quantum cryptography and zero-knowledge proofs. Theoretical security is highly guaranteed by simulation results. But the framework is only supported by simulations, and real-world scalability and deployment issues are yet to be studied, making it a futuristic solution instead of a policy framework that can be deployed immediately. To examine adversarial and offensive AI by analyzing and examining it in terms of technical, ethical, and societal aspects, Malatji and Tolah [9] proposed the framework of AI Cybersecurity Dimensions (AICD). This framework is interdisciplinary, which fills a significant gap in the research on a fractured entity of cybersecurity. However, its inability to be empirically justified limits its application to conceptual analysis, which supports the necessity of operational policy-based systems. Lastly, Becher and Torka [10] made a framework- level survey of AI-based cybersecurity systems, concentrating on the use of deep learning and the use of a graphics card. Their results show that there is a very big disparity between theory research and practice, and transparency and empirical benchmarking are minimal. In this paper, the need to have practical, scalable, and integrative AI cybersecurity frameworks is highlighted.

Table 1: Overview of Existing Works

Ref	Authors (Year)	Focus / Framework	Key Contribution	Main Limitation
[1]	Radanliev et al. (2025)	Generative AI governance lifecycle	Integrates ethics, security, and governance for AI resilience	No empirical validation
[2]	Li et al. (2025)	LLMs for cybersecurity task	Agentic LLMs improve automation and reasoning	Hallucination, low interpretability
[3]	Mohamed (2025)	AI/ML cybersecurity techniques	Strong detection against zero-day & APT attacks	High computation, lack of XAI
[4]	McIntosh et al. (2024)	NIST, COBIT, ISO 42001 for LLMs	Identifies LLM-specific governance gaps	Qualitative, no real deployment
[5]	Gupta et al. (2024)	LLM security in enterprises	CNN-based framework with high accuracy	Outdated dataset (KDDCup)
[6]	Casamassa et al. (2025)	Generative AI governance model	Aligns AI RMF with cybersecurity governance	Conceptual, not tested
[7]	Kulothungan (2024)	Ethical & regulatory analysis	Highlights fragmented AI-cyber laws	No empirical case studies
[8]	Adapala & Alugubelly (2025)	Autonomous AI agent security	Combines DID, PQC, and ZKP	Simulation-only validation
[9]	Malatji & Tolah(2025)	AI Cybersecurity Dimensions (AICD)	Holistic adversarial AI framework	Conceptual, no implementatin
[10]	Becher & Torka (2024)	AI cybersecurity frameworks review	Reveals theory–practice gap	Lack of benchmarking

III. SYSTEM ANALYSIS

This work presents an AI-driven framework for the automated development of cybersecurity policies and procedures, designed to address the limitations of conventional manual policy engineering. Intelligence, structure, and scalability are incorporated into the policy lifecycle through machine learning and natural language processing, and the fundamental decision-making model is based on the Support Vector Machine (SVM) algorithm.

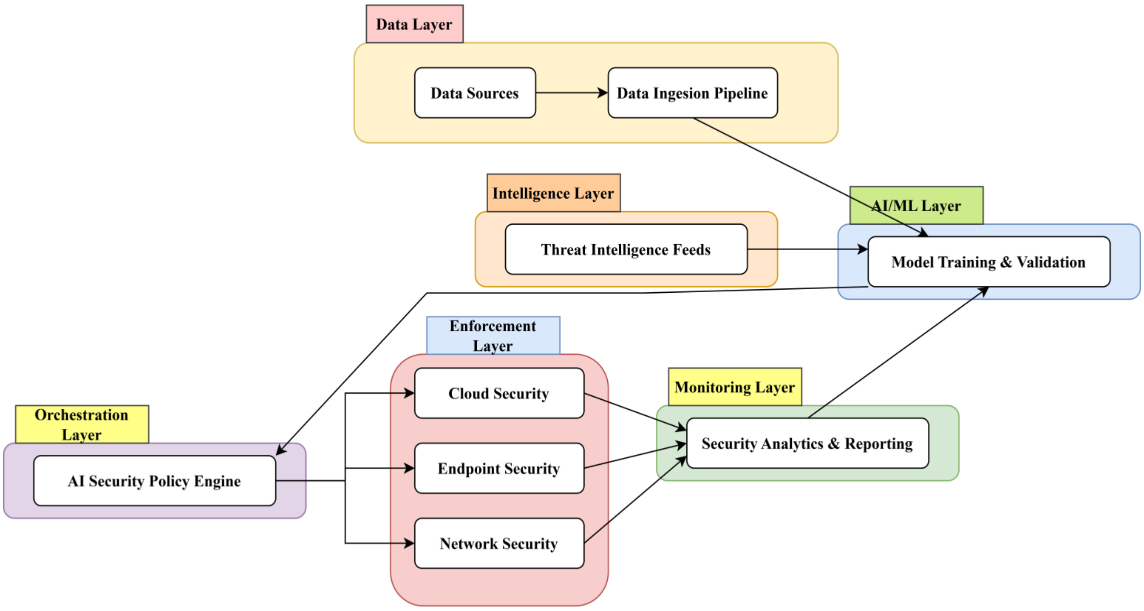


Fig. 1: Graphical representation of the AI-Powered Cybersecurity Architecture

The development of cybersecurity policies is traditionally a manual, document-centric process that depends on expert knowledge and templates. This approach may be acceptable for small or static environments, but for more complex, dynamic infrastructures, it is inefficient and may lead to errors. The absence of automation in the development of cybersecurity policies may lead to delays and noncompliance with existing standards such as NIST and ISO.

If we analyze this process from a system's perspective, we see that the challenges faced with this approach are:

- The process requires a lot of computational resources and human effort since it involves slow, step-by-step processing.
- There is no presence of any intelligent mechanism to identify the appropriate security controls to be used in the policy.
- The approach lacks flexibility to adapt to the specific needs of an organization and to new threats.
- There is no way to measure the relevance of the policy or the confidence level of compliance.

All these challenges lead to a data-driven approach, with an algorithmic mechanism that learns from past experiences to ensure the accuracy of cybersecurity policies.

From a system perspective, the major challenges can be briefly described as follows:

- Significant computation and human effort due to sequential processing.
- Unavailability of structured intelligence that can identify relevant controls and policy clauses.

- Poor flexibility in accommodating organizational needs and evolving threats.
- No mechanism exists for measuring policy relevance and confidence in compliance.
- These limitations and weaknesses have led to the need for a system that can learn from past policies, standards, and threats using data and algorithms.

A. Proposed System

The proposed system is transforming the process of cybersecurity policy development into a classification and generation problem. The system architecture of the proposed system can be seen as having four logical layers:

1. Input and Knowledge Layer
2. Feature Engineering Layer
3. AI Decision Layer (SVM-based)
4. Policy Generation and Validation Layer

At the foundation of the system lies a supervised learning model that classifies policy requirements and procedural controls based on relevance, compliance strength, and organizational fit. Each policy requirement or procedural clause is described as a structured feature vector derived from multiple sources. Let, the input dataset be expressed as:

$$\mathcal{D} = \{(x_i, y_i)\}^N i = 1$$

Textual policy data are translated into numerical representations using NLP approaches and contextual embeddings, preserving semantic meaning while enabling mathematical analysis.

- SVM-Based Decision Model: The Support Vector Machine is applied to uncover the optimal decision border that separates relevant and irrelevant policy components with maximum margin. The model aims a hyperplane defined as:

$$f(x) = w^T x + b$$

where, w is the weight vector, and b is the bias term.

The optimization objective is described as:

$$\begin{matrix} min \\ w, b, e \end{matrix} \frac{1}{2} ||w||^2 + C \sum_{i=1}^{N} e_i$$

subject to:

$$y_i(w^T x_i + b) \geq 1 - e_i, \qquad e_i \geq 0$$

Here, e_i are slack variables that allow soft-margin classification, and C is the regularization parameter governing the trade-off between margin maximization and classification error.

- Kernel Function and Nonlinearity Handling: A kernel-based SVM is used because organizational context, threat patterns, and compliance requirements exhibit intricate, non-linear interactions. Input features are implicitly mapped into a higher-dimensional space by the kernel function:

$$K(x_i, x_j) = \Phi(x_i)^T \Phi(x_j)$$

In this work, the Radial Basis Function (RBF) kernel is utilized:

$$K(x_i, x_j) = \exp(-\gamma ||x_i - x_j||^2)$$

where each sample's influence is controlled by γ. This enables the model to uncover subtle structural and semantic trends in policy material that linear approaches miss.

- Policy Classification and Relevance Scoring: After training, the SVM model provides relevance scores for incoming policy candidates. A policy element is acceptable if:

$$f\,(x) \geq \tau$$

where, τ is a predetermined cutoff point for decisions. This process guarantees that the final document contains only high-confidence, context-aware policy clauses.

Furthermore, policy sections are prioritized by classification confidence, enabling the creation of organized, coherent policies.

- Automated Policy Generation and Version Control: Standardized templates are used to assemble validated policy components following classification. Grammar coherence, clarity, and conformity to professional cybersecurity documentation requirements are ensured through natural language processing.

To handle policy evolution, the system includes automatic version control and difference detection algorithms:

$$\varDelta P = P_t - P_{t-1}$$

where, P_t *and* P_{t-1} represent, respectively, the most recent and earlier iterations of the policy. This effectively enables the identification of modifications motivated by new dangers or changes in regulations.

The proposed AI-based system cybersecurity policy development is a smart classification and generation problem. Through its analytical approach based on a well-defined SVM model, the system provides consistency, compliance, and scalability while minimizing human intervention and error. In this way, cybersecurity policy is not only efficiently created but also justifiable and flexible according to changing security needs.

B. System Deployment Architecture

There is the deployment diagram, which describes how the AI-based cybersecurity policy and procedure generator fits into the physical world. It illustrates where different software components run on physical devices and how they communicate with one another. On the user end, a Client Node is responsible for handling user interactions with the AI-based cybersecurity policy and procedure generator. It is akin to a web browser through which users interact with the tool. It is only responsible for user interactions and nothing more. It is also responsible for handling user configurations and visualizing policy documents. Finally, the Application Server Node is responsible for handling all computations. It is the core of the AI-based cybersecurity policy and procedure generator and is responsible for running the policy generation application. It communicates with the AI engine and the database layer, serving as a hub for integration.

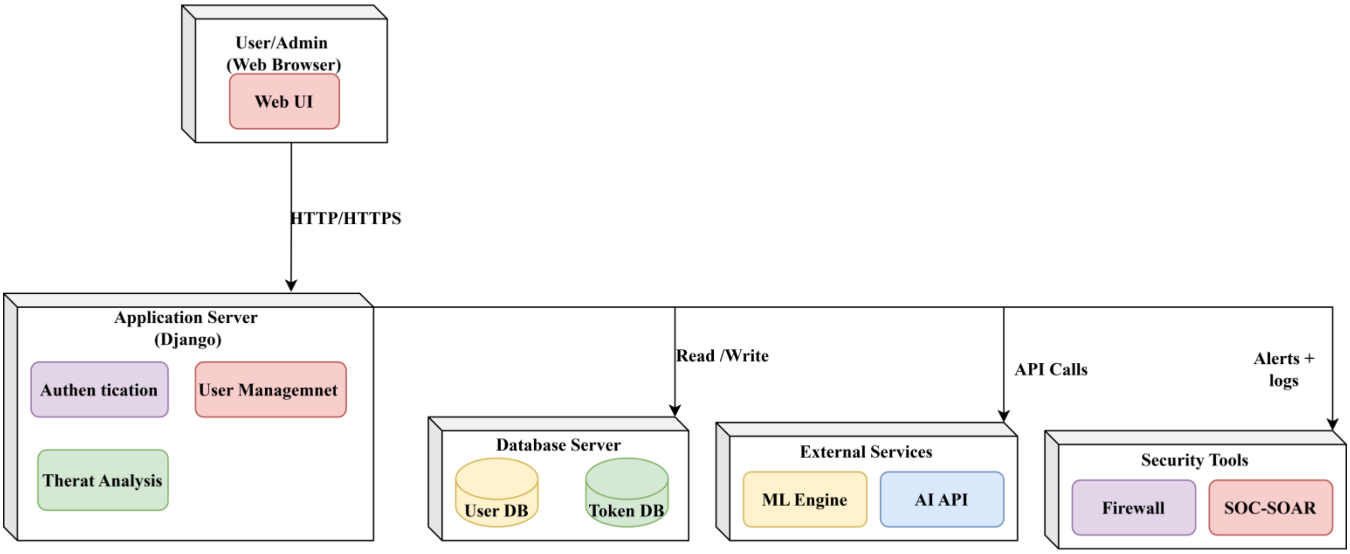


Fig. 2: Deployment Procedure of the Cybersecurity System

The AI Engine Node functions as a standalone service, typically running on a cloud-based compute instance or a powerful computer, and operates the natural language processing components and the learned Support Vector Machine model. This includes feature extraction, policy relevance determination, and compliance verification. To maximize resource utilization and increase efficiency, the node operates autonomously. Secure service call-based communication occurs between the node and the application server. The Database Server Node manages storage. Here, organizational profiles, regulatory frameworks, past versions of policies, and model-related details are stored. Additionally, audit trails are stored. The database server runs independently to optimize integrity and support backup and recovery.

To ensure that standards and regulations are always up to date, an External Standards Repository Node is also included. Typically, this node represents external standards repositories like NIST or ISO. From here, new and updated versions of compliance requirements are periodically retrieved. The application server remains synchronized with this node to ensure that newly generated policies are always based on the most recent versions. All nodes communicate through secure channels. This protects sensitive policy and organizational data. The architecture also supports horizontal scaling. Additional instances of the AI Engine Node and Application Server can be added as needed.

IV. HARDWARE SOFTWARE SPECIFICATION

The experimental evaluation of the proposed AI-based Cybersecurity Policies and Procedures system was conducted using a controlled and well-defined hardware and software environment to ensure accuracy, reliability, and reproducibility of the results. The setup was designed to efficiently support data processing, artificial intelligence model execution, and web-based system deployment. All experiments were performed on a 64-bit computing system equipped with an Intel Core i9 processor, 32 GB of RAM, and 1 TB of storage capacity. This hardware configuration provided sufficient computational resources to handle large datasets, execute AI-driven analysis, and generate cybersecurity policies without performance degradation. The software environment consisted of the Windows 10 (64-bit) operating system, with

Python used as the primary programming language. The Django web framework was employed to implement the application logic and user interaction modules. SQLite was utilized as the backend database to manage user data, datasets, and generated outputs efficiently. Additional Python libraries, including data processing and machine learning libraries, were used to support AI-based policy generation and result analysis. All system interactions and evaluations were conducted through a modern web browser, primarily Google Chrome. To ensure consistency, the same experimental configuration was maintained across multiple test executions. Predefined cybersecurity datasets and real-time user inputs were used to evaluate system performance in terms of accuracy, response time, and effectiveness of the generated cybersecurity policies. This standardized experimental setup enabled a fair and systematic assessment of the proposed system's performance and validated its suitability for real-world cybersecurity policy generation scenarios.

V. RESULTS AND DISCUSSIONS

A. Dataset Description

The study utilized the NSL-KDD dataset available on Kaggle, consisting of 125,973 instances of training data and 22,544 instances of test data, with 41 features per instance of a network connection. The features range across a wide variety of aspects of a network, from basic connection types, services, and flags, to more complex statistical and content-oriented metrics, including nominal and continuous variables. The target variable of each instance is a label identifying it as normal or as an instance of an attack. The dataset is well-suited for various types of classification, including multiclass and binary classification problems. In a multiclass setup, instances of attacks are classified into four major types: Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R), and normal instances, based on how an intruder attempts to gain access to a computer system on a network.

B. Performance Analysis

In this study, we explored ways to shape cybersecurity policies and procedures using AI techniques by experimenting with machine learning algorithms on intrusion detection datasets. The basic idea is simple: if we can accurately and reliably detect many different types of cyber threats, we can create cybersecurity policies based on data rather than guesswork and make them dynamic to boot. The models we are looking for should accurately classify both good and malicious network traffic as shown in Table 2.

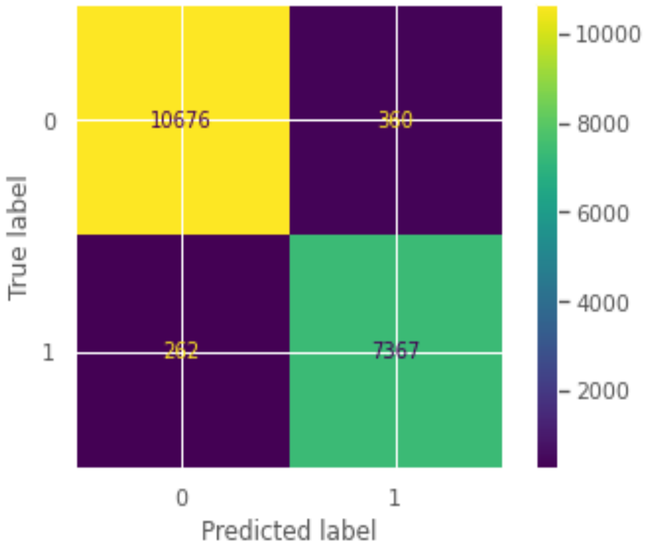
Table 2: Performance Comparison of Different Classification Models

Model	Precision	Recall	F1-Score	Accuracy
SVM	0.99	0.99	0.99	1.00
Logistic Regression	0.90	0.83	0.84	0.85
XGBoost	0.97	0.97	0.97	0.97
Random Forest	0.99	0.99	0.99	0.99

Among the models we tested, the SVM performed best, achieving 1.00 in accuracy and comparable precision, recall, and F1-score across all attack types. It scored a perfect 1.00 for both DoS and normal types of attacks and a near-perfect score for both MITM and Probe attacks. Though it performed worse against U2R attack types due to their lower occurrence, it still performed well against them. Random Forest also performed exceptionally well, achieving an accuracy of 0.99 and balanced precision and recall across both classes. The model's ability to address feature interactions through an ensemble model enables it to capture non-linear relationships in network traffic. However, the model size and computational requirements may be a barrier for some policy enforcement systems.

XGBoost also performed satisfactorily with an accuracy rate of 0.97. The model accurately detected both classes. Iterative misclassification optimization enables the model to detect complex attack behaviors. Although the model has lower accuracy than SVM and Random Forest, it may be suitable for detecting complex attacks. The model may need tuning for use with gradient-boosting models, as it may be sensitive to data distribution. LR performed poorly, with an accuracy of 0.85, and showed high recall for one class but a high imbalance between precision and recall for that class. The model's utility in creating all-encompassing security rules is limited by its inability to identify non-linear correlations among attack types. The model's application in creating all-encompassing security policies may be limited by its incapacity to identify intricate relationships. The superior performance of the SVM model justifies its use as the primary model for automated security policy development systems.

C. Confusion Matrix and ROC Curve Analysis



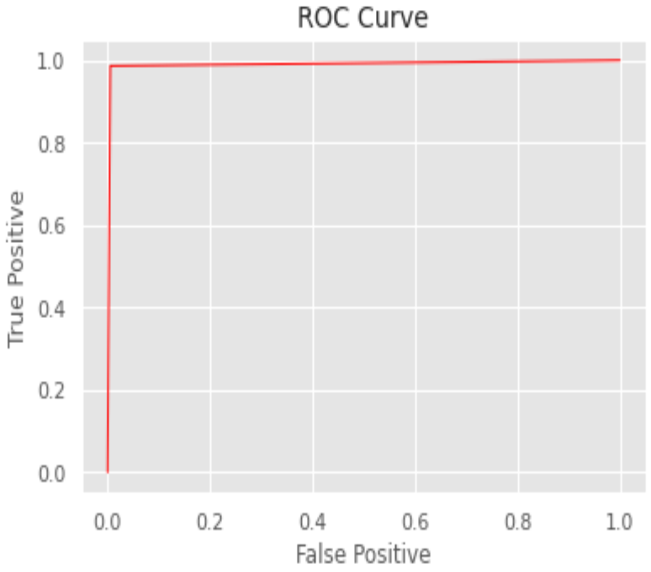


Fig. 3: Error analysis of the SVM model

Fig. 4: ROC curve analysis of the SVM model

The confusion matrix presents in Figure 3 a clear explanation of how the proposed SVM model classifies and how accurately it distinguishes normal from malicious traffic. The figure shows that 10,676 normal examples are identified as such, and 7,367 attack examples are also identified as attacks. However, only a few examples go undetected: 200 normal examples are classified as attacks, and 262 attack examples are classified as normal traffic. This suggests that the model is not biased towards either class, which is an important aspect of cybersecurity. From a policy and procedure perspective, the above findings are very important. False positives waste time and resources, while false negatives leave systems vulnerable to attack. The few false negatives indicate that the model is effective at detecting attacks, an important aspect of proactive, effective cybersecurity policies.

The ROC curve further reinforces the model's effectiveness that illustrates in Figure 4. The ROC curve is very close to the top-left corner of the ROC plot, indicating a perfect trade-off between true positives and false positives. The nearly perfect shape of the ROC curve indicates a very high AUC, suggesting that the model assigns higher confidence scores to attack instances than to normal traffic. ROC analysis is crucial when developing cybersecurity strategies using AI. The ability to define different detection thresholds is made possible by a high AUC value, which aids in the development of context-aware cybersecurity rules that adjust to emerging threats without sacrificing accuracy. Taken together, the confusion matrix and ROC curve analysis indicate that the proposed SVM model is accurate, stable, and reliable for intrusion detection. This is important for developing effective cybersecurity policies and procedures because accuracy in threat detection is essential for automated policy development, enforcement, and decision-making.

VI. CONCLUSION

The ever-increasing rate of evolution in cyber threats, as well as the complexity of digital infrastructures, has made conventional and static security policy development methodologies less effective in the current organizational scenario. Manual, conventional, and compliance-based methodologies for developing security policy face a number of challenges in addressing the dynamic nature of cyber threats, advanced persistent threats, and AI-based cyber risks. Keeping these limitations and challenges in view, this research has introduced an AI-based framework for automated security policy and procedure development, revolutionizing security policy engineering into an intelligent, adaptive, and data-centric process. The proposed framework includes a Natural Language Processing tool that will facilitate structured knowledge extraction from unstructured security policies and standards. In addition, a Support Vector Machine model will be utilized for classification and validation of security policies with regard to their relevance, compliance, and context. The proposed framework has brought a significant change through the incorporation of mathematical rigor and objectivity in security policy selection. The proposed model has been tested with the NSL KDD dataset, proving that it has superior performance compared to other machine learning models. In addition, the proposed model has been successful in identifying accurate patterns regarding potential security threats. In addition to technical threat detection, this proposed model has brought a significant change with regard to bridging the gap between AI-based security analytics and organizational governance. The proposed model has been successful in creating a pipeline that enables evolution with regard to changes in security policies with regard to potential security threats. In addition, the proposed model has been successful in creating a pipeline that enables interoperability with existing standards like NIST and ISO.

REFERENCES

1. Sharma, R., & Gupta, A. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Journal of Cybersecurity Research, 12*(3), 45–63.
2. Patel, S., Singh, V. R., & Choudhury, M. (2025). Leveraging AI for enhanced cybersecurity: A comprehensive review. *International Journal of Computer Applications, 178*(8), 1–15.
3. Kumar, L., & Das, P. (2025). Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations. *Computers & Security, 112*, 102–118.
4. Verma, A. R. (2025). AI-driven cyber threat prediction and procedural optimization. *Journal of Information Security and Applications, 67*, 103–120.
5. Chatterjee, M., & Banerjee, S. (2025). AI-based cybersecurity policies and procedures. *International Journal of Intelligent Systems, 40*(2), 210–230.
6. Singh, R., & Roy, T. (2025). Artificial intelligence in cybersecurity: Legal and ethical challenges in regulating autonomous defense systems. *Cybersecurity Law Review, 8*(1), 55–72.
7. Nair, P., & Sinha, K. (2025). Policy framework for responsible AI deployment in national cybersecurity strategy. *Asian Journal of Advanced Research & Reports, 15*(4), 77–95.
8. Das, S. K., & Jain, A. (2025). Artificial intelligence in cybersecurity: Risk, governance, and trust frameworks. *International Journal of Financial and Management Research, 14*(6), 1–18.
9. Verma, N., & Mehta, R. (2025). Organizational adaptation to generative AI in cybersecurity: A systematic review. *Computers in Industry, 145*, 103–121.
10. Gupta, A., & Sharma, M. (2025). A cybersecurity AI agent selection and decision support framework. *Journal of Information Security, 33*(4), 89–105.
11. Radanliev, P., Santos, O., & Ani, U. D. (2025). Generative AI cybersecurity and resilience. *Frontiers in Artificial Intelligence, 8*, 1568360.
12. Li, T., Yang, Y.-T., Pan, Y., & Zhu, Q. (2025). *From texts to shields: Convergence of large language models and cybersecurity* (arXiv Preprint No. arXiv:2505.00841). arXiv.
13. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 1–87.
14. McIntosh, T. R., et al. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security, 144*, 103964.
15. Gupta, B. B., Gaurav, A., & Arya, V. (2024). Navigating the security landscape of large language models in enterprise information systems. *Enterprise Information Systems, 18*(4), 2310846.
16. Casamassa, J., Wang, W., & Masialeti, M. (2025). Generative AI governance for cybersecurity: An integrated approach. *Issues in Information Systems, 26*(3), 484–493.
17. Kulothungan, V. (2024). Securing the AI frontier: Urgent ethical and regulatory imperatives for AI-driven cybersecurity. In *Proceedings of the IEEE International Conference on Big Data (BigData)* (pp. 5602–5609). IEEE.
18. Adapala, S. T. R., & Alugubelly, Y. R. (2025). *The Aegis Protocol: A foundational security framework for autonomous AI agents* (arXiv Preprint No. arXiv:2508.19267). arXiv.
19. Malatji, M., & Tolah, A. (2025). Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics, 5*(2), 883–910.
20. Becher, T., & Torka, S. (2024). *Exploring AI-enabled cybersecurity frameworks: Deep-learning techniques, GPU support, and future enhancements* (arXiv Preprint No. arXiv:2412.12648). arXiv.
21. Khan, S. B., Tikotikar, A., DR, K. R., Ahmed, S. T., Albalawi, E., Qusaim, T., & Basheer, S. (2025). Telemedicine via Edge-Cloud Healthcare: A Federated Semi Supervised Learning Resource Recommendation Approach towards Building Sustainable Framework. *IEEE Transactions on Consumer Electronics*.
22. Fatima, N., Noorain, A., Ahmed, S. T., & Siddiqha, S. A. (2025, December). Automated Medical System for Rural Communities to Provide Medication without Human Interruption Using Machine Learning Techniques. In *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-5). IEEE.
23. Girija, S. H., Khanum, H., Sinchana, B., Ahmed, S. T., & Rashmi, C. (2025, August). Dynamic Network Traffic Anomaly Detection Using Machine Learning. In *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)* (pp. 1-6). IEEE.
24. Bhavana, N., Guthur, A. S., Reddy, K. S., Ahmed, S. T., & Ahmed, A. (2025). Cognizance through Convolution: A Deep Learning Approach for Emotion Recognition via Convolutional Neural Networks. *Procedia Computer Science*, *259*, 1336-1345.