ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

Policies and Procedures for Cybersecurity Led by AI

[1]Mr. P.S. Rama Krishna, [2] V. Mohana Venkata Kavya,[3]Shaik Shajiya, [4]Pemmani Akhila,

[1]Associate Professor, Dept.of CSE, Rajamahendri Institute of Engineering & Technology, Bhoopalapatnam, Near Pidimgoyyi,Rajahmundry,E.G.Dist.A.P. 533107.

[2,3,4] Students,Dept.of CSE, Rajamahendri Institute of Engineering & Technology, Bhoopalapatnam, Near Pidimgoyyi,Rajahmundry,E.G.Dist.A.P. 533107.

Abstract—

The use of artificial intelligence (AI) in cyber security [1] has proven to be very effective as it helps security professionals better understand, examine, and evaluate possible risks and mitigate them. It also provides guidelines to implement solutions to protect assets and safeguard the technology used. As cyber threats continue to evolve in complexity and scope, and as international standards continuously get updated, the need to generate new policies or update existing ones efficiently and easily has increased [1][2]. The use of (AI) in developing cybersecurity policies and procedures can be key in assuring the correctness and effectiveness of these policies as this is one of the needs for both private organizations and governmental agencies. This study sheds light on the power of AI-driven mechanisms in enhancing digital defense procedures by providing a deep implementation of how AI can aid in generating policies quickly and to the needed level.

INTRODUCTION

The first and most effective line of defense against ever-changing cyber threats is a set of well-written, strictly enforced, and audited security policies and procedures [2][3]. The dangers that may arise from not regularly applying and auditing these security rules are defined in addition to their scope, standards, implementation instructions, roles, and duties. Some policies are derived from industry frameworks that standardize best practices and standards, while others are based on various aspects connected to the organization's structure. Develop, maintain, and enforce cyber security policies to be implemented and revised every defined period depending on various parameters, such as the newly published standards, as industry best practices are constantly evolving with new standards published by national institutions like the National Institute of Standards and Technology (NIST), Cybersecurity Maturity Model Certification (CMMC) [4], and the International Organization for Standardization (ISO). In order to effectively generate cyber security regulations, artificial intelligence (AI) can multitask and evaluate several datasets simultaneously. The preferences, size, and infrastructure of the enterprises make up one dataset, while the standardized control suggestions from published frameworks make up the other.

Artificial intelligence (AI) can analyze these two datasets and provide useful results for policymakers to use in reducing risks and responding appropriately to incidents [5]. Additionally, it may assess the organization's security posture, find areas that need improvement, and provide a strategy for implementing the identified faults and vulnerabilities. Utilizing technologies like as intrusion detection systems, firewalls, access control systems, and authentication procedures, AI may automate the enforcement of policy implementation once it has generated the desired rules. [6]

II. SECURITY POLICIES

A. What is a security policy?

Both technological and nontechnical assets should be protected by an organization's cyber security policy [2][7]. In addition to outlining potential dangers to resources, it lays forth rules and procedures to keep them and the organization safe. For optimal efficiency and practicability, security policies are often drafted in tandem with execution procedures. The policy and procedure outline the norms and responsibilities for carrying them out and keeping tabs on them. In order to foster accountability for the policy's implementation and comprehension of the potential damage caused by various security breaches, it is necessary to establish a list of duties and give a risk register. Part B: What exactly is a hacker threat? According to several regulatory

bodies, a security risk is the probability that an event may occur that might lead to the theft or compromise of an organization's assets. An additional metric for risk is the potential effect of the scenario on the designated assets. Reputation and identity, in addition to data and technology, may be considered assets. Alternatively, security risks might be described as a set of undiscovered vulnerabilities with a high potential of causing damage at certain future dates. What is the purpose of a security policy (C)? An organization's information security rules may be effectively established and maintained with the help of cyber security policies. Confidential information, intellectual property, physical equipment, and other assets are safeguarded by these rules. The possibility of data theft or damage caused by illegal access to these assets may be mitigated by policies. It is also difficult to quantify and evaluate cyber security concerns. Security policies aid in the detection and evaluation of cyber security hazards by establishing procedures that enable enterprises to efficiently lessen the impact of such risks. When operational teams have clear security procedures in place, they can respond quickly and effectively to any security breach. For an effective and rapid reaction to a security issue, policies will specify what to do, who to contact, and what data to record.

III. SECURITY FRAMEWORKS

When it comes to cybersecurity, organizations may benefit from security frameworks—also called cybersecurity frameworks or security standards—which are organized collections of best practices, rules, suggestions, and controls. In order to do business with the government, some firms are required to have certain certifications. [4] [9] Section A. Frameworks Created by ISO. If your company is seeking for a complete framework to secure your data via rules and processes, go no further than the International Organization for Standardization (ISO). Two of the most well-known standards for managing information security are ISO 27001 and ISO 27002 [9]. To guarantee that companies take the necessary steps to be secure and compliant, the two standards provide concepts and methods. Organizations may safeguard their networks according to the precise recommendations provided by ISO standards, which include topics such as access control, incident response, asset management, and business continuity. It aids in maintaining a safe atmosphere for the IT and security departments as well. B. NIST Frameworks. In order to help businesses identify and prevent cyber vulnerabilities and safeguard their digital assets from potential cyberattacks, the US federal agency known as the National Institute of Standards and Technology (NIST) [9] regularly creates and publishes standard recommendations and guidelines. Although some commercial organizations used the published standards to guarantee digital security and compliance with government requirements, NIST frameworks were originally developed for usage by federal agencies. Many small and medium-sized businesses rely on NIST standards, like NIST 800-171, when formulating their security policies. For systems and organizations outside of the federal government, it lays forth the security requirements for protecting Controlled Unclassified Information (CUI). Out of the fourteen domains that make up NIST 800-171, the two most crucial are access control (AC) and incident response (IR). At its heart, cyber security operation teams are responsible for these two areas, which need extensive regulations. Section C. NIST System for the Management of AI Risks. The National Institute of Standards and Technology (NIST) has released a new framework, the AI Risk Management Framework (AI RMF), to aid businesses and people in effectively mitigating AI-related risks. This model lays out the many dangers that could arise from relying on AI technologies [10][11]. Because of these dangers, implementing AI isn't easy, and we need to think of further measures to make sure we don't do any of them and lessen the impact of the others.

IV. GENERATING POLICIES USING AI

A. Objective.

The primary objective of this project is to explore and implement the use of Artificial Intelligence (AI) to streamline the development and enhancement of cybersecurity policies and procedures. With cyber threats becoming increasingly sophisticated, traditional approaches to policy creation are often too slow or outdated by the time they are deployed. This project aims to harness the capabilities of AI to automate and optimize the formulation of cybersecurity strategies, ensuring that they are both timely and responsive to emerging digital threats.

One key goal is to develop a system that can intelligently analyze current cybersecurity trends, threat intelligence data, and compliance requirements to assist in drafting precise and effective policy documents. By doing so, the project addresses a critical challenge faced by organizations: the gap between threat identification and policy response. The integration of machine learning models and natural language processing (NLP) will allow the system to interpret complex data, learn from past incidents, and provide structured policy suggestions

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

that are aligned with industry best practices and international standards.

Another important objective is to reduce the workload on cybersecurity professionals by automating repetitive and data-heavy tasks involved in policy generation. This will allow experts to focus more on strategic planning and risk management rather than spending time on manual policy drafting and compliance updates. The system will also feature adaptability, allowing it to update existing policies automatically in response to new threats or changes in compliance laws, minimizing human error and ensuring continued protection.

The project also aims to bridge the gap between technical and non-technical stakeholders by generating policies that are understandable, actionable, and easily interpretable. This ensures that policies are not just technically sound but also effectively implemented across all departments in an organization. AI-driven tools will enable better communication, quicker training, and more efficient policy enforcement through intelligent document generation and semantic analysis of existing protocols.

Ultimately, this project seeks to demonstrate how AI can be a transformative force in the field of cybersecurity governance. By enabling faster, smarter, and more effective policy creation, it lays the foundation for proactive cyber defense mechanisms in both private and public sectors. Through this initiative, the long-term goal is to contribute to a more secure digital ecosystem where policies evolve as swiftly as the threats they are designed to combat. Lastly, there are other uses for these security strategies, such as creating training and awareness materials. This training prevents a variety of hazards stemming from many sources, such social engineering, and guarantees that the whole business is prepared. Section E. The Use of AI. In order to parse the organization dataset that was specified earlier and the selected security framework, the AI integration module is built once the policy generation objectives and needs are determined. The built module automatically fills up the preset security policy fields and interfaces with Open AI 4.0 over an Integration REST object. With the help of the organization information and the regulation dataset, the module may create a custom prompt. After that, the Open AI API is queried, and the policy dataset is returned in its original format. The parameters used to interface with the API are shown in Table 1.

TABLE I. API PARAMETERS

API Parameters	
Parameter Name	*Parameter Value*
API Model	GPT-4
Max_tokens	2500
Temperature	0.8

In order to interface with GTP-4, this designed module is run and the outcomes are evaluated. For the most effective policy and guideline production, the prompt was revised many times. We used the two datasets you supplied to develop these policies. A review of the list of duties and an analysis of the policies that were established were conducted. For the purpose of managing and addressing any and all AI risks, the whole process was updated in comparison to the NIST AI RMF framework. G. Showcase. Use of the suggested module with the NIST 800-171 and ISO 27001/27002 control sets, as well as aggregated data on the organization's infrastructure and operational scale, demonstrates its efficacy. Each control has its own structured policy that is generated by communication with GPT-4, the most powerful API from OpenAI. Scope, policy, procedure, roles and responsibilities, risk register, and, where relevant, auditing or measuring variables were all effectively produced. In order to create a set of policies and procedures, the created process is run over all eleventy-one controls and fourteen domains outlined in NIST 800-171. After that, the rules and procedures are organized to create a comprehensive security guideline document that the IT and security operation teams may refer to. Assuming all goes according to plan, this will provide an extra safeguard and guarantee conformity with NIST standards. Results demonstrated consistent adaptation to various changes in the organization and the newly published controls, and the developed policies are updated frequently via simulation. G. Outcomes. In order to create policies with all the necessary fields, the module analyzes the organization profile and control needs. After going over the organized rules and processes, we were able to record the following: Result policies are not excessively technical but stated in simple language so that everyone can understand them. Policies are in line with the organization's aims and objectives, according to the results. • Adherence: All policies that are developed comply with the control's rules

and regulations. The policies that are created are enforced to make sure that everyone is following them, thanks to the defined roles and duties. • Ongoing Reviews: The policies that are developed are dynamic and are evaluated on a frequent basis to accommodate evolving risks. • Coherence: The findings demonstrate that the policies are in line with one another and with the organization's overall security framework.• Aims that can be measured: indicators for measuring the efficacy of measures are included in all policies that are developed. After testing, the application efficiently creates a cybersecurity policy for the NIST 800-171 Access Control domain for a ten-person firm that oversees the tax administration for real estate companies on the administrative area of their website. For each of the following subjects, we requested that the client fill out a form: • Data and system classification • Organizational structure and information Access Control Procedures • Tools and Vendors • User Authentication and Authorization The data was organized according to the NIST 800-171 framework's standards, and the AI API integration produced the access control security policy. The created Access Control Policy demonstrates a reliable approach that the business may use to safeguard important real estate tax records. Following the concept of least privilege, this policy lays forth the duties and obligations. It is mandatory for all workers to use multi-factor authentication for user authentication and permission. Access is now given according to reorganized job responsibilities. In addition to including quantifiable targets for ongoing improvement, the produced policy backs uniformity across security recommendations.

V. CONCLUSION

Lots of work goes into developing security policies and processes, but if they aren't done well, organizations risk having security holes in their systems. Artificial intelligence demonstrates its worth as a tool for assisting in the formulation of such policies. Updating and revising these rules on a regular basis and making sure they align with newly issued frameworks also helps to maintain them on a high quality. Using artificial intelligence (AI) and pre-existing APIs, this article lays out a process for creating cyber security rules that take into account both internal company preferences and external ISO/NIST requirements. After some tweaks and analysis, the produced policies proved to be quite beneficial. Chapter Six: What Comes Next An essential weapon in the battle against security vulnerabilities will be the security policies that are created and updated. But these regulations, like everything else in the operational sector, need auditing and monitoring. Additional ways to audit the created policies' application and ensure control and monitoring of the security operation teams may be developed from this study.

REFERENCES

[1] A. Mehra and S. Badotra, "Artificial Intelligence Enabled CyberSecurity," *2021 6th International Conference on Signal Processing,Computing and Control (ISPCC)*, Solan, India, 2021, pp. 572-575, doi:10.1109/ISPCC53510.2021.9609376.
[2] Cisco Systems. (2008b). Data leakage worldwide: The effectiveness ofcorporate security policies. Retrieved May 12, 2011, from World WideWeb:http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/Cisco-STL-Data-Leakage-2008-.pdf
[3] L. Li, W. He, L. Xu, A. Ivan, M. Anwar and X. Yuan, "Does ExplicitInformation Security Policy Affect Employees' Cyber Security Behavior?A Pilot Study," *2014 Enterprise Systems Conference*, Shanghai,China, 2014, pp. 169-173, doi: 10.1109/ES.2014.66.
[4] V. Sundararajan, A. Ghodousi and J. E. Dietz, "The Most CommonControl Deficiencies in CMMC non-compliant DoD contractors," *2022IEEE International Symposium on Technologies for Homeland Security(HST)*, Boston, MA, USA, 2022, pp. 1-7, doi:10.1109/HST56032.2022.10025445.
[5] W. Matsuda, M. Fujimoto, T. Aoyama and T. Mitsunaga, "Cyber SecurityRisk Assessment on Industry 4.0 using ICS testbed with AI and Cloud,"*2019 IEEE Conference on Application, Information and Network Security(AINS)*, Pulau Pinang, Malaysia, 2019, pp. 54-59, doi:10.1109/AINS47559.2019.8968698.
[6] J. C. Haass, "Cyber Threat Intelligence and Machine Learning," *2022Fourth International Conference on Transdisciplinary AI (TransAI)*,Laguna Hills, CA, USA, 2022, pp. 156-159, doi:10.1109/TransAI54797.2022.00033.
[7] I. Ellefsen, "The development of a cyber security policy in developingregions and the impact on stakeholders," 2014 IST-Africa Conference Proceedings, Pointe aux Piments, Mauritius, 2014, pp. 1-10, doi:10.1109/ISTAFRICA.2014.6880605.
[8] R. Mishina, S. Tanimoto, H. Goromaru, H. Sato and A. Kanai, "RiskManagement of Silent Cyber Risks in Consideration of Emerging Risks,"*2021 10th International Congress on Advanced Applied Informatics(IIAI-AAI)*, Niigata, Japan, 2021, pp. 710-716, doi: 10.1109/IIAIAAI53430.2021.00126.

[9] P. P. Roy, "A High-Level Comparison between the NIST Cyber SecurityFramework and the ISO 27001 Information Security Standard," 2020National Conference on Emerging Trends on Sustainable Technology andEngineering Applications (NCETSTEA), Durgapur, India, 2020, pp. 1-3,doi: 10.1109/NCETSTEA48365.2020.9119914.

[10]Swarnalata, Dr. Sridevi Garapati, Dr. Sujatha Peetala, & Dr. Rambabu Rampatruni. (2024). Artificial intelligence, its knowledge, attitude, and perceptions among future health care workforce - undergraduates in a government medical college. *Journal of Population Therapeutics and Clinical Pharmacology*, *31*(11), 1452-1462. https://doi.org/10.53555/dp2d4308

[11] National Institute of Standards and Technology. "AI Risk ManagementFramework." NIST January 26, 2023. Available online:https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[12] A. Martin-Lopez, "AI-Driven Web API Testing," 2020 IEEE/ACM 42nd International Conference on Software Engineering: CompanionProceedings (ICSE-Companion), Seoul, Korea (South), 2020, pp. 202-205.

[13] S. Tjoa, P. K. M. Temper, M. Temper, J. Zanol, M. Wagner and A.Holzinger, "AIRMan: An Artificial Intelligence (AI) Risk ManagementSystem," *2022 International Conference on Advanced EnterpriseInformation System (AEIS)*, London, United Kingdom, 2022, pp. 72-81,doi: 10.1109/AEIS59450.2022.00017.

[14] M. T. Siponen, "Analysis of modern IS security development approaches:towards the next generation of social and adaptable ISS methods",Information and organization, 15, 4, 2005, 339-375

[15] M. Warner, "Notes on the Evolution of Computer Security Policy in theUS Government, 1965-2003," in *IEEE Annals of the History ofComputing*, vol. 37, no. 2, pp. 8-18, Apr.-June 2015, doi:10.1109/MAHC.2015.25.