

# AI-DRIVEN CYBERSECURITY POLICY AND PROCEDURE DEVELOPMENT

G.Harshith<sup>1</sup>, J.V.M Sharanya<sup>2</sup> P.Sahasri<sup>3</sup>, Goski Sathish<sup>4</sup>

<sup>1,2,3</sup> UG Scholar, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

<sup>4</sup>Assistant Professor, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

[harshith3030@gmail.com](mailto:harshith3030@gmail.com)

## Abstract:

The use of artificial intelligence (AI) in cyber security 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. 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. The current approach to developing cybersecurity policies and procedures is characterized by several significant drawbacks. First, it is time-consuming and labor-intensive, requiring organizations to invest substantial time and effort to create these policies manually. This process often results in inconsistency and human error, as manually crafted documents may lack uniformity across different sections or departments, potentially leaving gaps in security coverage. Additionally, the rapid evolution of cyber threats and industry standards makes it challenging to keep policies up-to-date, which can leave organizations vulnerable to emerging risks. Lastly, the manual nature of policy development limits scalability, making it difficult to create comprehensive policies for larger organizations or complex systems, and increases the likelihood of oversight. Furthermore, without automated cross-referencing, policies may deviate from established industry frameworks like NIST or ISO, jeopardizing compliance efforts. The use of standardized inputs ensures consistency and accuracy across generated policies, aligning them with industry best practices. It enhances efficiency and speed by allowing the AI system to quickly process multiple datasets simultaneously, drastically reducing the time and effort required for policy creation.

## 1.INTRODUCTION

A brain computer interface (BCI) is a system that lets you control a computer with your thoughts. The basic idea is to use technology to read your brainwaves and interpret what you're thinking. Then, the computer can do what you want it to do. Brain-Computer Interfaces (BCIs) are currently in their nascent phase of development, yet their potential to transform our interaction methods is immense technology. There are a few different ways to build a BCI. One is to use electrodes that are implanted in the brain. Another is to use sensors that sit on the surface of the skull. The most common way to measure brainwaves is with an electroencephalograph (EEG). EEGs

measure the electrical activity of the brain and are often used in research. BCI research is ongoing, and several different applications are being explored. It has been possible to identify the kind of sensations that are hiding beneath the surface using a variety of methods and techniques, such as: Due to its reliable results, Electroencephalography (EEG) is widely used in the field of emotion recognition (ER) from facial expression, voice intonation, and signal from the Autonomic Nervous System (ANS) like heart rate and Galvanic Skin Response (GSR). It is also widely used because it is simple to record and reasonably priced.

Emotion classification from EEG waves requires some techniques and procedures. One of these processes involves recording and then preprocessing raw signals. After cleaning up the dataset and organizing the data, the best feature is extracted and evaluated using machine Learning or deep learning techniques. Step by step machine learning with end to end deep learning are the two primary machine learning approaches for EEG signal analysis.

ML also known as conventional machine learning, is characterized by its sequential nature, with the three primary stages consisting of preprocessing, feature extraction, and feature categorization using machine learning algorithms. However, it's hard to keep up with manual extraction, and the equations for (TD and FD) are full of complexity and noise (such as electromyography), so machine learning techniques are dubious. To get around this, researchers turned to deep learning, which favors an end-to-end approach.

The system utilizes deep learning techniques to analyze these data points, focusing on features such as arousal, valence, and dominance. The EEG signals are processed using various methods to remove noise and artifacts, ensuring the data is clean and suitable for model training.

Security policies and procedures are the first and most efficient defense layer against evolving cyber threats if correctly written, well enforced into action plans, and periodically audited. These security policies define the scope, guidelines, implementation instructions, roles, and responsibilities, along with possible risks if not applied and audited periodically. Typically, policies are developed based on multiple factors that are related to the organization's structure, and others are based on the industry frameworks standardizing best practices and standards. As the industry best practices are evolving with new standards periodically published by national institutions like the National Institute of Standards and Technology (NIST), Cybersecurity Maturity Model Certification (CMMC), and International Organization for Standardization (ISO), cyber security policies should be developed, maintained, and enforced to be implemented and revised every defined period depending on different parameters such as the newly published standards. Artificial Intelligence (AI) has the capability of processing more than one

dataset at the same time and in a productive way to produce cyber security policies efficiently. One dataset can be the organizations' preferences, size, and infrastructure, while the other can be the standardized recommendations of the controls as set in the published standard frameworks. AI can process these two datasets and generate appropriate outputs to be used in developing policies that can limit risks and ensure correct incident responses. It can also locate potential flaws and vulnerabilities, evaluate the organizations' security posture, identify what needs improvement, and finally generate an action plan for implementation. After generating the requested policies, AI can also be used to automate the enforcement of their implementation through technologies like intrusion detection systems, firewalls, access control systems, and authentication mechanisms.

## 2. LITERATURE SURVEY

### Literature Survey for AI-Driven Cybersecurity Policy and Procedure Development

The use of artificial intelligence (AI) in cyber security 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. Artificial Intelligence Enabled Cyber Security

In recent years, the integration of Artificial Intelligence (AI) in cybersecurity has garnered significant attention due to its potential to enhance the detection, prevention, and response to cyber threats. The 2021 6th International Conference on Signal Processing, Computing, and Control (ISPPCC) highlights advancements in AI-driven cybersecurity solutions. AI techniques such as machine learning, deep learning, and natural language processing are being employed to analyze vast amounts of data, identify patterns, and predict potential security breaches in real-time. These AI models improve the accuracy of threat detection, mitigate the risks posed by evolving cyber-attacks, and automate incident responses, significantly bolstering cybersecurity frameworks.

#### 2. Cisco Systems. Data leakage worldwide: The effectiveness of corporate security policies.

Data leakage has become a critical global concern, with increasing incidents compromising sensitive information across various industries. The effectiveness of corporate security policies plays a crucial role in mitigating such risks. Research shows that well-implemented policies, including data encryption, access control, and employee training, can significantly reduce vulnerabilities. However, the rapid evolution of cyber threats and the rise of remote work have exposed gaps in traditional security approaches. Studies highlight that while many organizations adopt robust policies, the lack of continuous monitoring, policy enforcement, and adaptation to new attack vectors often undermines their effectiveness, leading to persistent data leakage challenges worldwide.

#### 3. Does Explicit Information Security Policy Affect Employees

Research on the impact of explicit information security policies on employees' cybersecurity behavior suggests that clear, well-communicated policies can significantly influence how employees adhere to security practices. A pilot study on this topic indicates that when employees are aware of specific security guidelines, they are more likely to engage in protective behaviors such as using strong passwords, avoiding phishing scams, and following data protection protocols. However, the study also emphasizes that the mere existence of a security policy is not enough. The effectiveness depends on factors such as policy clarity, organizational culture, and continuous training. Employees' understanding and perception of these policies play a critical role in shaping their cyber hygiene and reducing human-related security vulnerabilities.

#### 4. The Most Common Control Deficiencies in CMMC non-compliant DoD contractors

The Cybersecurity Maturity Model Certification (CMMC) was developed to enhance the security posture of contractors working with the U.S. Department of Defense (DoD). Research on common control deficiencies among non-compliant contractors reveals recurring issues that hinder certification. Key deficiencies include inadequate access control, insufficient incident response planning, lack of multi-factor authentication, and poor system monitoring practices. Additionally, many contractors struggle with properly securing sensitive data, enforcing encryption standards, and maintaining regular security audits. These gaps indicate a broader challenge in aligning contractor cybersecurity practices with CMMC requirements, often due to limited resources or misunderstanding of compliance obligations, which leaves critical DoD information vulnerable to cyber threats.

#### 5. Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud

The integration of Industry 4.0 technologies, such as the Industrial Control Systems (ICS), artificial intelligence (AI), and cloud computing, has transformed industrial operations but also introduced new cybersecurity risks. Studies utilizing ICS testbeds for cybersecurity risk assessment in Industry 4.0 environments emphasize the need for enhanced security measures to address these risks. AI-driven models are being employed to detect anomalies and predict potential cyber threats in real time, while cloud-based solutions offer scalable security management. However, research highlights vulnerabilities in data transmission, cloud infrastructure, and remote access, which can be exploited by cyber-attacks. These assessments provide critical insights into developing robust, AI-powered cybersecurity frameworks that can effectively safeguard Industry 4.0 systems against emerging threats. Organizations are investing a lot of time and effort to develop their security policies and procedures which if not developed correctly, will lead to security vulnerabilities. AI proves itself as an effective mechanism to help generate these policies. It also helps to keep these policies on high standards and up to date, periodically revised and synchronized with the new published frameworks.

## 3. PROPOSED METHODOLOGY

The proposed AI-driven approach to generating cybersecurity policies and procedures offers a range of significant advantages. Primarily, it enhances efficiency and speed by allowing the AI system to quickly process multiple datasets simultaneously, drastically reducing the time and effort required for policy creation. The use of standardized inputs ensures consistency and accuracy across generated policies, aligning them with industry best practices.

The use of standardized inputs ensures consistency and accuracy across generated policies, aligning them with industry best practices. Additionally, the system is adaptable and customizable, taking into account organization-specific parameters such as infrastructure, size, and culture, which enables it to produce tailored policies that meet the unique needs of each organization. This AI-driven system is scalable, easily accommodating policy generation for organizations of varying sizes and complexities, from small businesses to large

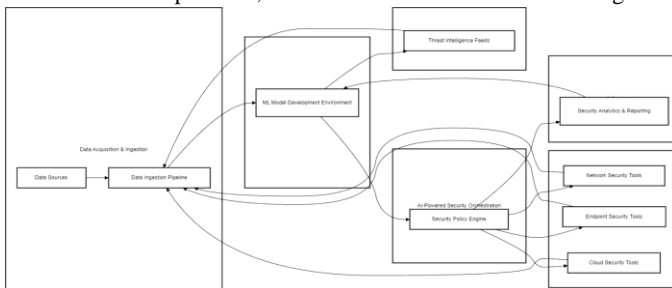


Figure 1: Proposed system.

The system follows a structured approach: The proposed AI-driven approach to generating cybersecurity policies and procedures offers a range of significant advantages. Primarily, it enhances efficiency and speed by allowing the AI system to quickly process multiple datasets simultaneously, drastically reducing the time and effort required for policy creation. The use of standardized inputs ensures consistency and accuracy across generated policies, aligning them with industry best practices. Additionally, the system is adaptable and customizable, taking into account organization-specific parameters such as infrastructure, size, and culture, which enables it to produce tailored policies that meet the unique needs of each organization. It also automates compliance by integrating the latest industry standards (e.g., NIST, ISO) into the policy generation process, ensuring that the resulting documents adhere to current regulations. Finally, this AI-driven system is scalable, easily accommodating policy generation for organizations of varying sizes and complexities, from small businesses to large enterprises with diverse technology stacks. Parallel processing of multiple datasets is a technique used to speed up data-intensive tasks by breaking down a large workload into smaller, independent sub-tasks that can be executed simultaneously on multiple processors or machines. This method is especially useful when processing large volumes of data or performing computationally intensive operations, such as data transformation, analysis, or machine learning model training. Let's elaborate on each step of the Parallel Processing of Multiple Datasets process:

#### Step 1. Preprocessing and Dataset Preparation

**Step Description:** Before parallel processing begins, it's essential to pre the data, h process and prepare your datasets.

This includes cleaning and handling missing values, transforming the data (e.g., normalizing, encoding), and splitting large datasets into manageable chunks for parallel execution.

**Example:** If you're processing sales data, preprocessing might involve: Removing duplicate entries. Filling in missing values or handling outliers. Splitting the data into subsets based on time periods, regions, or product categories

**Importance in Parallel Processing:** Properly prepared data ensures that each parallel task gets a clean, consistent, and manageable subset of data, reducing the risk of errors during processing.

#### Step 2. Define Task Granularity

**Step Description:** Task granularity refers to how finely tasks are divided for parallel execution. It determines whether the tasks will be small and fine-grained (many tasks) or large and coarse-grained (fewer tasks).

**Example:** If you're processing customer transactions:

**Fine-Grained Granularity:** You might divide the data into smaller, transaction-level chunks and process each one independently across parallel tasks.

**Coarse-Grained Granularity:** You could process transactions grouped by customer or by region, resulting in fewer, larger chunks.

**Importance in Parallel Processing:** Choosing the appropriate task granularity is critical for balancing the workload across available processors. Fine-grained tasks might introduce high overhead due to excessive task management, while coarse-grained tasks might not fully utilize available resources. Proper granularity ensures efficient parallel processing without wasting resources.

#### Step 3. Parallelization Strategy

**Step Description:** Once the granularity of the tasks is defined, the parallelization strategy determines how the tasks will be executed in parallel. It involves selecting the parallelization method (e.g., data parallelism, task parallelism) and how tasks will be distributed across available processors or nodes.

**Example:** If you're analyzing data from a large retail database:

**Data Parallelism:** You could distribute subsets of the data (e.g., by store or time period) across multiple processing units, where each unit performs the same analysis on its data.

**Task Parallelism:** Different tasks, such as data preprocessing, feature extraction, and model training, could be executed concurrently on separate processors or machines.

**Importance in Parallel Processing:** The parallelization strategy determines how efficiently tasks are executed concurrently. A well-defined strategy maximizes resource utilization and minimizes delays due to task dependencies. A poorly designed strategy can lead to imbalance, where some processors are idle while others are overloaded.

#### Step 4. Parallel Execution

**Step Description:** Parallel execution refers to the actual running of tasks concurrently. This step involves distributing the defined tasks across available computing units (e.g., CPU cores, nodes, GPUs) and ensuring that each unit works on its assigned task without unnecessary delays.

**Example:** For a machine learning application Distributed Execution: If using a distributed system like Apache Spark, tasks can be distributed across different nodes in a cluster to process large datasets in parallel. Multi-core Execution: On a single machine, tasks might be distributed across multiple CPU cores or GPUs for faster computation.

**Importance in Parallel Processing:** Efficient parallel execution



ensures that tasks are processed concurrently, reducing the overall computation time. It's crucial for maximizing the utilization of available hardware, such as multi-core processors or distributed computing environments, thereby improving performance.

#### Step 5. Handling Data Synchronization and Communication

**Step Description:** When tasks are executed in parallel, they often need to communicate and synchronize their progress, especially in distributed systems. This step involves ensuring that data consistency is maintained, tasks that depend on each other can exchange information, and any shared resources are handled correctly.

**Example:** If you're processing customer feedback data: **Synchronization:** Ensuring that one task does not overwrite or conflict with another task when updating shared resources (e.g., aggregated statistics).

**Merging Results:** Combine the processed sales statistics (e.g., total sales, average sales per region) from each parallel task. **Post-Processing:** You might apply final transformations, like aggregating regional sales to generate a nationwide total or calculating performance metrics like sales growth.

**Importance in Parallel Processing:** Post-processing and result integration ensure that the output of parallel tasks is meaningful and accurate. Without careful result merging, partial results might not align correctly, leading to errors in the final output.

#### Step 7. Error Handling and Fault Tolerance

**Step Description:** Error handling and fault tolerance ensure that the parallel processing system can recover from failures, such as task crashes or resource unavailability. This step involves detecting errors, managing task retries, and handling failures gracefully.

**Example:** In a large distributed system: **Error Detection:** If a node fails to process its assigned data, the system detects the failure and marks the task as incomplete. **Fault Tolerance:** The system can reschedule the failed task on another node or retry it from a checkpoint.

**Importance in Parallel Processing:** Robust error handling and fault tolerance prevent data loss or corruption in the event of hardware or software failures. This ensures that parallel processing can continue without significant disruption and produces reliable, consistent results.

#### Step 8. Output and Cleanup

**Step Description:** After parallel tasks are completed, the results are written to the desired output location, and any resources used during execution are cleaned up. This includes closing files, freeing memory, and releasing other system resources.

**Example:** For a data analysis task: **Output:** The final results of the parallel tasks (e.g., cleaned datasets, statistical analysis) are written to output files or databases. **Cleanup:** Unused resources such as memory, threads, or temporary files are properly released to avoid system resource leaks.

**Importance in Parallel Processing:** Output and cleanup ensure that resources are efficiently managed and that no lingering processes or files cause issues. Proper cleanup also avoids memory leaks and ensures that the system remains responsive for future tasks. Additionally, ensuring output integrity guarantees that results are accessible and correct.

## 4.EXPERIMENTAL ANALYSIS

Figure 2: Home Page

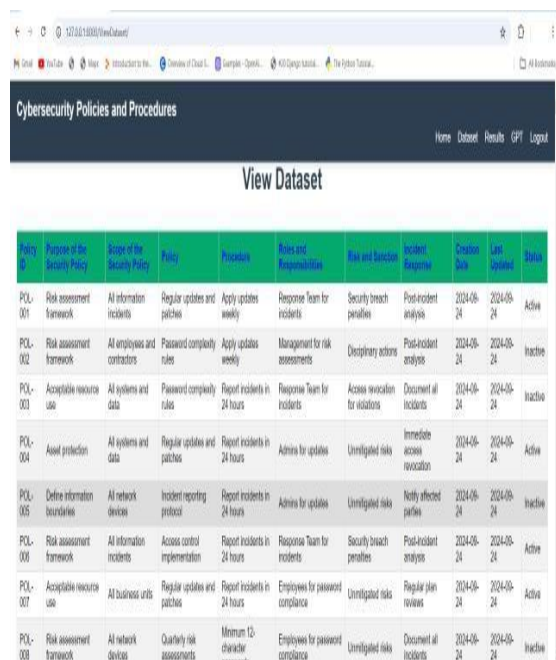
**Communication:** In a distributed setup, nodes might need to share intermediate results, like sending partial sums back to a central node for final aggregation.

**Importance in Parallel Processing:** Synchronization and communication are crucial to avoid data inconsistencies and race conditions. Without proper synchronization, tasks might overwrite results, or some tasks might complete before others, leading to incorrect outputs. Efficient communication ensures that tasks work together seamlessly.

#### Step 6. Post-Processing and Result Integration

**Step Description:** After parallel tasks are completed, the results need to be aggregated, combined, and possibly further processed to generate the final output. This step ensures that the individual outputs of parallel tasks are merged correctly and useful insights are extracted.

**Example:** If you processed sales data by region in parallel:



Policy ID	Purpose of the Security Policy	Scope of the Security Policy	Policy	Procedures	Roles and Responsibilities	Risk and Severity	Incident Response	Creation Date	Last Updated	Status
POL-001	Risk assessment framework	All information incidents	Regular updates and patches	Apply updates weekly	Response Team for incidents	Security breach penalties	Post-incident analysis	2024-06-24	2024-06-24	Active
POL-002	Risk assessment framework	All employees and contractors	Password complexity rules	Apply updates weekly	Management for risk assessments	Disciplinary actions	Post-incident analysis	2024-06-24	2024-06-24	Inactive
POL-003	Acceptable resource use	All systems and data	Password complexity rules	Report incidents in 24 hours	Response Team for incidents	Access revocation for violations	Document all incidents	2024-06-24	2024-06-24	Inactive
POL-004	Asset protection	All systems and data	Regular updates and patches	Report incidents in 24 hours	Admins for updates	Unmitigated risks	Immediate access revocation	2024-06-24	2024-06-24	Active
POL-005	Define information boundaries	All network devices	Incident reporting protocol	Report incidents in 24 hours	Admins for updates	Unmitigated risks	Notify affected parties	2024-06-24	2024-06-24	Inactive
POL-006	Risk assessment framework	All information incidents	Access control implementation	Report incidents in 24 hours	Response Team for incidents	Security breach penalties	Post-incident analysis	2024-06-24	2024-06-24	Active
POL-007	Acceptable resource use	All business units	Regular updates and patches	Report incidents in 24 hours	Employees for password compliance	Unmitigated risks	Regular plan reviews	2024-06-24	2024-06-24	Active
POL-008	Risk assessment framework	All network devices	Quarterly risk assessments	Minimum 12-character passwords	Employees for password compliance	Unmitigated risks	Document all incidents	2024-06-24	2024-06-24	Inactive

Figure 3: GPT Test

Figure 4: Dataset

The project says AI-driven cybersecurity architecture integrates machine learning (ML) and security tools to enhance threat detection and response. The system begins with data acquisition from various sources such as network logs, system logs, and cloud security events, which are processed through the data ingestion pipeline. The ingested data is then utilized by an ML model development environment to train machine learning models for detecting anomalies and potential threats. Additionally, external threat intelligence feeds provide real-time insights to improve security analysis. At the core of this framework is the AI-powered security orchestration, managed by a security policy engine that analyzes incoming data and



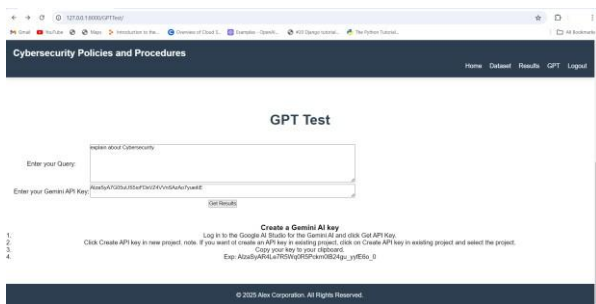
enforces security policies. The security enforcement layer consists of network security tools, endpoint security tools, and cloud security tools, which receive inputs from the policy engine to mitigate threats. Security analytics and reporting provide real-time insights and alerts for security teams to monitor and respond effectively. By integrating AI and automation, this architecture enhances cybersecurity operations, reduces response time, and improves overall threat detection capabilities.

## CONCLUSION

Organizations are investing a lot of time and effort to develop their security policies and procedures which if not developed

## REFERENCES

- [1] National Institute of Standards and Technology. "AI Risk Management Framework." NIST January 26, 2023. Available online: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.
- [2] V. Sundararajan, A. Ghodousi and J. E. Dietz, "The Most Common Control Deficiencies in CMMC non-compliant DoD contractors," 2022 IEEE International Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 2022, pp. 1-7, doi: 10.1109/HST56032.2022.10025445.



- [3] S. Tjoa, P. K. M. Temper, M. Temper, J. Zanol, M. Wagner
- [5] J. C. Haass, "Cyber Threat Intelligence and Machine Learning," 2022 Fourth International Conference on Transdisciplinary AI (TransAI), Laguna Hills, CA, USA, 2022,

- [6] A. Mehra and S. Badotra, "Artificial Intelligence Enabled Cyber Security," 2021 6th (ISPC), Solan, India, 2021,

ISSN: 1934-9955 [www.ijise.net](http://www.ijise.net)

Vol-20 Issue-01 April 2025

correctly, will lead to security vulnerabilities. AI proves itself as an effective mechanism to help generate these policies. It also helps to keep these policies on high standards and up to date, periodically revised and synchronized with the new published frameworks. This paper defines a mechanism of using AI through developed APIs to generate cyber security policies based on organizational preferences on one side and ISO / NIST standards on the other side. The generated policies were revised and analyzed, and results showed that they are highly effective.

- and A. Holzinger, "AIRMan: An Artificial Intelligence (AI) Risk Management System," 2022 International Conference on Advanced Enterprise Information System (AEIS), London, United Kingdom, 2022, pp. 72-81, doi: 10.1109/AEIS59450.2022.00017.
- [4] A. Martin-Lopez, "AI-Driven Web API Testing," 2020