American Journal of Multidisciplinary Research and Innovation (AJMRI)

ISSN: 2158-8155 (ONLINE), 2832-4854 (PRINT)

VOLUME 4 ISSUE 3 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Multidisciplinary Research and Innovation (AJMRI)

Volume 4 Issue 4, Year 2025
ISSN: 2158-8155 (Online), 2832-4854 (Print)
DOI: https://doi.org/10.54536/ajmri.v4i4.4823
https://journals.e-palli.com/home/index.php/ajmri

Improving Cyber Security in Power Systems and Substation Automation Using Intelligent Based System

Chukwuagu M. Ifeanyi[1*], Ogbu Gregory[2], Chukwu Linus[2]

Article Information

Received: March 18, 2025

Accepted: Aprli 24, 2025

Published: June 24, 2025

Keywords

Social Studies, Technology Integration, Phenomenology, Qualitative, In-Depth Interview, Focus Group Discussion, Thematic Analysis, Tagum City, Philippines

ABSTRACT

The constant failure in cyber security in power systems and substation automation that has crippled business activities that mostly depend on power to run their routine activities are caused by Lack of Adequate Security Measures, Human Error, Outdated Software and Hardware, Insufficient Training and Awareness, Insider Threats, Weak Access Control Mechanisms, Inadequate Network Segmentation, Failure to Patch Vulnerabilities, Complexity of the System, Third-Party Vendor Risks and Denial of Service (DoS) Vulnerabilities. This is surmounted by introducing improved cyber security in power systems and substation automation using intelligent based system. To achieve this, it is done in this procedure characterizing and establishing the causes of failure in cyber security in power systems and substation automation, designing a SIMULINK model for cyber security in power systems and substation automation, designing a rule base that will reduce the causes of failure in cyber security in power systems and substation automation,training ANN in the rule base for effective reduction of causes of failure in cyber security in power systems and substation automation, developing an algorithm for the process, designing a SIMULINK model for improving cyber security in power systems and substation automation using intelligent based system and validating and justifying the percentage of improvement in the reduction of causes of failure in cyber security in power systems and substation automation. The results obtained were the conventional Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation was 25%. On the other hand, when an intelligent based system was incorporated into the system, it drastically reduce the cause failure in improving cyber security in power systems and substation automation to 21.53%, the conventional outdated software and hardware that cause failure in improving cyber security in power systems and substation automation was 15%. Meanwhile, when an intelligent based system was inculcated in the system, it became reduced to 12.92% thereby enhancing the performance of cyber security in power systems and substation automation by 2.08%, the conventional Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation was 8%. However, when an intelligent based system was integrated in the system, it was reduced to 6.9% and the conventional Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation was 2% while when an intelligent based system was incorporated in the system, it automatically reduced to 1.7%. Finally, with these results obtained, It vehemently shows that the percentage improvement in cyber security in power systems and substation automation was 0.3%.

INTRODUCTION

In recent years, the integration of intelligent technologies in power systems and substation automation has revolutionized the way modern grids are managed, controlled, and protected. However, this technological advancement has also exposed critical infrastructure to increased cyber threats and vulnerabilities. Power systems, being essential to national security and economic stability, require robust cyber security measures to prevent disruptions that could lead to widespread outages or damage to sensitive equipment. Traditional security methods, while effective to some extent, are no longer sufficient to address the complexity and sophistication of modern cyber attacks. This has led to the need for intelligent-based systems that leverage artificial intelligence (AI), machine learning (ML), and other advanced technologies to enhance cyber security in power systems and substation automation. By adopting intelligent systems, power grids can not only detect and respond to cyber threats in real time but also anticipate potential risks, thereby improving overall system resilience and operational stability. This paper explores the application of intelligent-based systems in bolstering cyber security within power systems and substation automation, highlighting their potential to safeguard critical infrastructure in an evolving threat landscape.

Problem Statement

The increasing digitization and automation of power systems, particularly through the adoption of smart grids and substation automation, have introduced new challenges in maintaining cyber security. Power systems

[1] Electrical/Electronic Engineering, Caritas Univeristy Amorj-Nike, Emene, Enugu State, Nigeria
[2] Mechanical Engineering & Production(Thermo-fuild), Enugu State Univeristy of Science and Technology (ESUT), Nigeria
[*] Corresponding author's e-mail: chukwuaguifeanyi35@gmail.com

are becoming more interconnected, and their reliance on information and communication technologies (ICT) has made them vulnerable to a wide range of cyber threats, including malware, phishing, denial of service (DoS) attacks, and more sophisticated targeted intrusions. These threats, if successful, could lead to system malfunctions, equipment damage, or even large-scale power outages, posing significant risks to national security and economic stability.

Traditional cyber security approaches in power systems are often insufficient to handle the complexity, scale, and evolving nature of modern cyber attacks. Moreover, the vast volume of data generated by power networks and substations requires advanced methods for detecting, analyzing, and mitigating threats in real time. This situation presents a critical need for a more dynamic, intelligent-based system that can adapt to new threats and proactively defend power systems against cyber attacks.

The problem, therefore, is how to improve the cyber security of power systems and substation automation by integrating intelligent-based systems that can not only detect and respond to cyber threats in real time but also anticipate future vulnerabilities and ensure the continued stability and reliability of the power grid.

Aim and Research Objectives

Aim

The aim of this research is to develop and implement intelligent-based systems to enhance cyber security in power systems and substation automation. By leveraging advanced technologies such as artificial intelligence (AI), machine learning (ML), and data analytics, the objective is to design a proactive cyber security framework capable of detecting, responding to, and mitigating cyber threats in real time. This approach seeks to improve the resilience, reliability, and security of power grid infrastructure, ensuring continuous and stable power supply while protecting critical assets from evolving cyber threats.

Research Objectives

1. To characterize and establish the causes of failure in cyber security in power systems and substation automation
2. To design a SIMULINK model for cyber security in power systems and substation automation
3. TO DESIGN A RULE BASE THAT WILL REDUCE THE CAUSES OF FAILURE in cyber security in power systems and substation automation
4. To train ANN in the rule base for effective reduction of CAUSES OF FAILURE in cyber security in power systems and substation automation
5. To develop an algorithm for the process
6. To design a SIMULINK model for improving cyber security in power systems and substation automation using intelligent based system
7. To validate and justify the percentage of improvement in the reduction of causes of FAILURE in cyber security in power systems and substation automation

The research objectives of Improving Cyber Security in Power Systems and Substation Automation Using Intelligent-Based System are as follows:

To analyze the current cyber security challenges in power systems and substation automation: This includes identifying key vulnerabilities and threats posed by increasing digitization and automation in power infrastructure.

To evaluate the limitations of traditional cyber security methods in protecting power systems: This involves assessing the adequacy of existing security frameworks in mitigating advanced cyber threats.

To develop an intelligent-based cyber security system for power systems and substation automation: This will focus on designing a system that integrates AI, machine learning, and data analytics to detect, respond to, and prevent cyber threats in real time.

To implement and test the intelligent-based system in simulated environments: The objective is to evaluate the system's effectiveness in identifying, responding to, and mitigating various cyber attacks within power systems.

To optimize the intelligent-based system for real-time threat detection and response: This involves fine-tuning the system to ensure it operates efficiently in dynamic and complex power grid environments.

To propose a framework for integrating intelligent cyber security solutions into existing power system infrastructure: This includes formulating recommendations for utilities and grid operators on how to adopt and deploy intelligent-based cyber security systems for enhanced protection.

To assess the impact of intelligent-based cyber security solutions on the reliability and stability of power systems: This objective aims to evaluate how the implementation of these technologies affects overall grid performance and resilience.

Scope of the work

The scope of this research focuses on the development and implementation of intelligent-based systems to improve cyber security in power systems and substation automation. Specifically, the study encompasses the following key areas:

Cyber Security Challenges in Power Systems and Substation Automation

The research will explore the unique vulnerabilities introduced by digitalization and automation, such as unauthorized access, malware, data breaches, and denial-of-service (DoS) attacks.

Traditional vs. Intelligent-Based Cyber Security Methods

The study will compare traditional cyber security methods with intelligent-based solutions, highlighting the limitations of current practices and the advantages of using AI, machine learning, and advanced analytics in threat detection and prevention.

Development of Intelligent-Based Cyber Security Framework

This research will focus on designing a system that integrates intelligent technologies to detect, respond to, and mitigate cyber threats in real time. The framework will be tailored to address the specific needs of power systems and substation automation.

Simulated Environment Testing

The intelligent-based cyber security framework will be tested in simulated environments to evaluate its effectiveness in identifying and mitigating various types of cyber attacks commonly associated with power systems.

Real-Time Threat Detection and Response

The study will focus on optimizing the intelligent-based system for real-time operations, ensuring that it can handle large volumes of data, detect anomalies, and respond swiftly to potential threats.

Framework Integration

The research will provide a detailed plan for integrating the intelligent-based cyber security system into existing power system infrastructure, ensuring compatibility and seamless operation alongside traditional systems.

Impact on Power System Stability and Reliability

The research will assess how the implementation of intelligent cyber security solutions affects the overall stability and reliability of power systems, ensuring that increased security does not compromise grid performance.

This study will not cover other forms of infrastructure outside the scope of power systems and substation automation, nor will it delve into physical security measures, focusing instead on cyber threats and intelligent countermeasures.

Scope

The scope of this research is centered on improving the cybersecurity of power systems and substation automation by utilizing intelligent-based systems. The research will address the following areas:

Cyber Security Threats in Power Systems

This includes exploring the specific cyber threats and vulnerabilities that impact power systems and substations, such as malware, phishing, data tampering, and denial-of-service (DoS) attacks.

Intelligent-Based Cyber Security Systems

The research will focus on the development and application of intelligent-based technologies, including artificial intelligence (AI), machine learning (ML), and data analytics, to enhance threat detection, response, and mitigation in power systems.

Comparison with Traditional Methods

The study will evaluate the limitations of traditional cybersecurity methods in power systems and assess the added value of intelligent-based approaches in addressing evolving cyber threats.

Design and Implementation

The research will focus on designing a cyber security framework that integrates intelligent technologies, tailored specifically to power systems and substation automation. This will involve creating algorithms and models capable of detecting and responding to cyber threats in real time.

Testing and Validation

The intelligent-based system will be tested and validated in a simulated environment to measure its effectiveness in detecting, preventing, and mitigating various cyber attacks.

Integration with Existing Infrastructure

The study will explore how to integrate intelligent cyber security systems into existing power grid infrastructures and substation automation setups, ensuring compatibility and minimal disruption.

Impact on System Performance

The research will analyze the impact of the intelligent-based system on the overall performance of the power grid, particularly its ability to maintain stability, reliability, and operational efficiency while enhancing cybersecurity.

Recommendations for Future Implementation

The research will provide recommendations on the adoption of intelligent cyber security solutions for power utilities, with a focus on scalability, cost-effectiveness, and sustainability.

The study is limited to cyber threats related to power systems and substation automation and will not cover physical security aspects or cyber security measures for unrelated sectors.

LITTERATURE REVIEW

Cyber Security Threats in Power Systems and Substation Automation

Power systems and substation automation are becoming increasingly vulnerable to cyberattacks due to the growing interconnection of control systems with information and communication technologies (ICT). Research has shown that cyber threats such as malware, distributed denial-of-service (DDoS) attacks, and unauthorized access can lead to significant disruptions in power systems, ranging from service interruptions to equipment damage and economic losses. In particular, substation automation systems, which play a critical role in monitoring and controlling the flow of electricity, are often targeted due to their importance in grid operation and their connection to supervisory control and data acquisition (SCADA) systems (Hahn *et al.*, 2013). As the complexity and scale of power grids increase, so do the potential attack surfaces, requiring robust cyber security solutions that can adapt to new threats.

Limitations of Traditional Cyber Security Methods

Traditional cyber security methods in power systems, such as firewalls, intrusion detection systems (IDS), and encryption, are often reactive and struggle to keep pace with the evolving landscape of cyber threats. These approaches are primarily rule-based and rely on predefined attack signatures, making them less effective against sophisticated and zero-day attacks that can bypass conventional security measures. Furthermore, power systems generate vast amounts of data, which makes real-time monitoring and threat detection challenging using manual or traditional methods (Mackiewicz, 2006). Studies have highlighted that the integration of these conventional security methods often lacks the agility needed to address advanced persistent threats (APTs) or insider threats that may not exhibit obvious malicious behavior until significant damage has been done (Cárdenas *et al.*, 2018).

Intelligent-Based Systems in Cyber Security

In recent years, the adoption of intelligent-based systems, leveraging artificial intelligence (AI) and machine learning (ML), has emerged as a promising solution to enhance cyber security in power systems and substation automation. AI and ML algorithms can analyze large datasets, detect patterns, and identify anomalies in real time, enabling power systems to detect potential cyber threats proactively. According to Zhang *et al.* (2016), intelligent-based systems can offer a dynamic, adaptive defense mechanism that goes beyond predefined rule sets, making them more capable of identifying previously unknown threats. Machine learning models, such as supervised learning, unsupervised learning, and deep learning, have been successfully applied to intrusion detection systems (IDS) in power grids, with a higher detection rate of anomalies compared to traditional methods (Mousavian & Masoum, 2018).

Application of AI and ML in Power System Cyber Security

The application of AI and ML in power system cyber security has been studied extensively, particularly in the context of enhancing substation automation. Researchers in Liu *et al.* (2011) demonstrated that AI-based systems can be used to automate the identification and classification of cyber threats in real time by analyzing traffic patterns within the communication network. In another study, AI-driven approaches were utilized to optimize the performance of intrusion detection systems, significantly improving their accuracy in detecting cyber attacks in substation automation systems (Pasqualetti *et al.*, 2013). These studies highlight the potential of intelligent-based systems to offer both real-time detection and automatic response capabilities, which are crucial for maintaining system stability in the face of cyber attacks.

Challenges in Implementing Intelligent-Based Cyber Security Systems

Despite the potential benefits, there are several challenges associated with implementing intelligent-based systems for cyber security in power systems. One major concern is the integration of AI and ML with legacy systems that may not be compatible with modern security solutions. The complexity of power system infrastructure, along with stringent reliability and availability requirements, means that any cyber security solution must be thoroughly tested to avoid unintended consequences, such as false positives or system downtime (Sridhar *et al.*, 2012). Additionally, the reliance on large datasets for training machine learning models can be problematic in environments where labeled data is scarce or inconsistent. These challenges underscore the need for continued research and development to create intelligent-based cyber security systems that are both effective and practical for real-world deployment in power systems.

Recent Advances and Future Directions

Recent advances in intelligent-based cyber security for power systems focus on developing hybrid approaches that combine multiple AI techniques with traditional security mechanisms. For example, Wei *et al.* (2017) introduced a hybrid model that integrates deep learning with traditional IDS, achieving higher accuracy in detecting complex cyber attacks while reducing false positives. Furthermore, the use of reinforcement learning to dynamically adjust security parameters based on real-time threat assessments has gained attention as a way to improve the adaptability of cyber security systems in power grids (Giani *et al.*, 2013). Future research is expected to focus on refining these hybrid models and exploring new AI techniques, such as federated learning, to enhance the privacy and scalability of intelligent-based cyber security solutions in power systems and substation automation.

The literature demonstrates that intelligent-based systems, particularly those using AI and ML, hold great promise for improving cyber security in power systems and substation automation. While traditional methods remain essential, their limitations in addressing sophisticated and emerging threats highlight the need for more advanced solutions. AI-driven cyber security systems offer a proactive and adaptive approach, enabling real-time threat detection and automated response, which are critical in maintaining the security and reliability of power infrastructure. However, challenges such as system integration and data availability must be addressed for widespread implementation. Continued research in hybrid models and the development of intelligent-based systems tailored to the unique needs of power grids will be key to future advancements in this field.

Research Gap

Despite significant advancements in intelligent systems and cybersecurity, there remains a significant research gap in the application of these technologies to enhance the security of power systems and substation automation. This gap stems from several factors, including:

Complex and Heterogeneous Environments

Power systems and substation automation systems are complex networks involving various interconnected components, protocols, and technologies. This heterogeneity makes it challenging to develop comprehensive and effective security solutions.

Real-Time Constraints

Power systems require real-time operations and decision-making. Intelligent-based systems must be able to process data and respond to threats in a timely manner without compromising system performance or reliability.

Evolving Threat Landscape

Cyber threats are constantly evolving, making it difficult to develop static security measures. Intelligent-based systems must be capable of adapting to new threats and vulnerabilities.

Data Privacy and Security

Power systems and substation automation systems handle sensitive data, such as customer information and operational data. Ensuring data privacy and security while leveraging intelligent-based systems is a critical challenge.

Integration with Existing Infrastructure

New security solutions must be seamlessly integrated with existing power system infrastructure without disrupting operations or incurring excessive costs.

Specific research areas that could address these gaps include:

- Development of advanced anomaly detection algorithms that can accurately identify cyber threats in real-time, even in the presence of noise and adversarial attacks.
- Application of machine learning techniques to automate the analysis of large volumes of network traffic and identify patterns indicative of malicious activity.
- Integration of blockchain technology to provide tamper-proof records of system events and enhance data integrity.
- Development of privacy-preserving data mining techniques that allow for the analysis of data without compromising sensitive information.
- Evaluation of the effectiveness of different intelligent-based security solutions in real-world power system environments.

By addressing these research gaps, it is possible to develop more effective and resilient cyber security solutions for power systems and substation automation, ensuring the reliability and security of critical infrastructure.

MATERIALS AND METHODS

Materials

The development of an intelligent-based system for improving cybersecurity in power systems and substation automation involves the use of various materials, both hardware and software, as well as specific methodologies and datasets. The key materials include:

Power System Infrastructure and Substation Automation Components

SCADA (Supervisory Control and Data Acquisition) Systems

SCADA systems are crucial in power systems and substation automation for real-time data acquisition, monitoring, and control of field devices.

Intelligent Electronic Devices (IEDs)

These are used to monitor and control substation equipment and play a critical role in system automation.

Phasor Measurement Units (PMUs)

PMUs are deployed in the grid to measure electrical waves and provide real-time data on the stability of power systems.

Communication Networks

Substation automation heavily relies on communication networks, such as Ethernet-based networks or IEC 61850 protocol, to transmit data between control centers and substations.

Cyber Security Hardware

Firewalls, routers, switches, and other network security hardware are essential for protecting the communication channels of the power system.

Cyber Security Software and Tools

Intrusion Detection Systems (IDS)

IDS tools are used to monitor and detect unauthorized access or anomalies within the network. These tools are critical for identifying potential cyber attacks.

Firewalls and Access Control Software

Firewalls are deployed to prevent unauthorized access, while access control mechanisms ensure only authorized personnel can access critical components of the power system.

Encryption Algorithms

Cryptographic software is used to secure communications within power systems and protect sensitive data from interception or manipulation.

Artificial Intelligence and Machine Learning Algorithms

AI and ML software, such as supervised learning, unsupervised learning, and deep learning models, are deployed to analyze network traffic, detect anomalies, and predict potential cyber threats.

Datasets and Simulation Platforms

Cyber Security Datasets

Historical and real-time data from power systems are used to train machine learning models. These datasets contain normal operational data and logs of cyber attacks, which are crucial for the system to learn and detect anomalies.

Simulated Power Grid Environments

Simulators, such as Grid LAB-D or Power World, are used to replicate real-world conditions of a power grid, allowing for the testing and validation of cyber security systems in a controlled environment.

Attack Simulation Tools

Tools like Metasploit or Kali Linux can be used to simulate cyber attacks on the network, enabling the evaluation of how well the intelligent-based system responds to threats.

Artificial Intelligence and Machine Learning Frameworks

Tensor Flow and PyTorch

These are widely used frameworks for developing and deploying machine learning and deep learning models. They allow for the creation of intelligent algorithms capable of detecting cyber threats in real time.

Scikit-Learn

A popular library for machine learning, Scikit-learn is useful for implementing various algorithms like classification, clustering, and anomaly detection to identify cyber security issues in power systems.

Reinforcement Learning Tools

Reinforcement learning libraries, such as OpenAI Gym, are used to develop models that can adaptively improve cyber security measures based on real-time interactions with the power grid.

Hardware for Computational Processing

High-Performance Servers and GPUs

Power system data is often large and requires significant computational resources for real-time analysis. High-performance servers equipped with GPUs are used to process machine learning models, especially for deep learning and complex algorithms.

Data Storage Solutions

Cloud-based storage or local data centers are required for managing the vast amounts of data generated by power systems and substation automation, enabling efficient data processing for cyber security monitoring.

Standards and Protocols

IEC 61850 Standard

This standard is used for communication protocols in substation automation systems. It defines the communication architecture, data models, and network configurations for ensuring secure data exchange between devices.

NIST Cyber Security Framework

The NIST framework provides guidelines for improving cyber security in critical infrastructure, including power systems. It serves as a reference for establishing security policies and best practices.

IEEE Standards

Various IEEE standards, such as IEEE 1686 (Substation Intelligent Electronic Devices Cyber Security Capabilities), offer guidelines for ensuring cybersecurity in substation automation systems.

User Interfaces and Visualization Tools

Security Information and Event Management (SIEM) Systems

SIEM systems are used to collect, analyze, and visualize data from various sources within the power grid to provide real-time visibility into security events.

Human-Machine Interfaces (HMIs)

HMIs allow operators to interact with the substation automation system, providing them with real-time data on grid performance and alerts on potential cyber security threats.

These materials collectively enable the design, development, and implementation of an intelligent-based cyber security system for power systems and substation automation. Through the integration of these tools and technologies, power grids can be made more secure against evolving cyber threats.

Methods

The methodology for improving cybersecurity in power systems and substation automation using an intelligent-based system involves several key phases, which include system analysis, data collection, model development, simulation, and testing. The steps below outline the approach used in this research.

System Analysis and Requirements Gathering

Review of Existing Power System Infrastructure

Analyze the current power system and substation automation setup, including communication protocols, network architecture, and control systems such as SCADA and Intelligent Electronic Devices (IEDs). This step helps to identify the critical assets and potential vulnerabilities that are most at risk from cyber attacks.

Cyber Security Threat Assessment

Conduct an analysis of potential cyber threats specific to power systems and substation automation, such as malware attacks, distributed denial-of-service (DDoS), and unauthorized access. This phase involves studying attack vectors and understanding how cyber incidents can affect system reliability.

Define Security Requirements

Establish cyber security goals and requirements, such as real-time threat detection, anomaly detection, system reliability, and response capabilities. These requirements form the foundation for the development of the intelligent-based system.

Data Collection and Preprocessing

Power System Data Collection

Collect historical and real-time operational data from the power system, including SCADA logs, IED traffic, and network communication patterns. This data is critical for training machine learning models.

Cybersecurity Incident Logs

Gather data related to past cyberattacks on power systems, including attack signatures, traffic anomalies, and system behavior during and after attacks. This data is used to classify normal versus malicious activity.

Preprocessing

Clean and preprocess the collected data by removing noise, handling missing values, and transforming it into formats suitable for machine learning algorithms. Feature extraction techniques are applied to select relevant parameters, such as communication traffic volume, device behavior, and protocol types.

Model Development Using Artificial Intelligence and Machine Learning

Machine Learning Model Selection

Choose appropriate machine learning models for threat detection and classification. Common models used include:

Supervised Learning Algorithms

Decision trees, support vector machines (SVM), and random forests are applied to classify known attack patterns.

Unsupervised Learning Algorithms

Clustering techniques such as k-means and DBSCAN are used to detect anomalies in network traffic that may indicate new or unknown cyber threats.

Deep Learning Models

Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can be used to process complex datasets, such as time-series data generated by power systems, for more accurate anomaly detection.

Algorithm Training

Train the chosen machine learning models using the preprocessed datasets. This involves splitting the data into training and testing sets, tuning hyper parameters, and using techniques such as cross-validation to ensure model accuracy and prevent over fitting.

Reinforcement Learning

Implement reinforcement learning techniques to enable the system to learn from real-time interactions with the power grid and improve its defense strategies dynamically based on evolving threats.

Development of Intelligent-Based Cyber Security Framework

Integration of AI with Existing Systems

Integrate the trained machine learning models with the existing power system and substation automation infrastructure. This involves configuring the AI models to monitor real-time data streams from SCADA systems, IEDs, and communication networks.

Real-Time Threat Detection

Develop an intelligent-based intrusion detection system (IDS) that leverages the machine learning models to detect anomalous behavior in real-time. The IDS continuously monitors network traffic, device communication, and system behavior for signs of cyberattacks.

Automated Response Mechanism

Create an automated response system that triggers predefined actions when a potential cyber threat is detected. This can include isolating affected systems, blocking malicious IP addresses, and alerting system operators to investigate further.

Simulation and Testing in a Controlled Environment

Simulated Environment Setup

Set up a simulated power system and substation automation environment using tools such as GridLAB-D or PowerWorld to replicate real-world operating conditions. The simulation includes SCADA systems, IEDs, communication networks, and typical cyber attacks.

Attack Scenarios

Simulate various cyber attacks, such as DDoS, man-in-the-middle attacks, and data tampering, to test the effectiveness of the intelligent-based system. These scenarios are designed to assess the system's ability to detect, respond to, and mitigate the threats in real-time.

Performance Evaluation

Evaluate the performance of the intelligent-based system based on key metrics such as detection accuracy, response time, false positive/negative rates, and overall system reliability. Compare the results to traditional cyber security methods to demonstrate the advantages of the intelligent-based approach.

Optimization and Deployment

Model Optimization

Based on the results of the simulation, fine-tune the machine learning models and algorithms to improve their accuracy and reduce false positives. Techniques such as hyper parameter tuning and ensemble learning can be employed for optimization.

System Integration

Integrate the optimized intelligent-based system into the actual power grid infrastructure. This involves configuring it to monitor real-time data streams from the live network and ensure that it operates effectively alongside existing cyber security solutions such as firewalls and encryption.

Ongoing Monitoring and Adaptation

Implement continuous monitoring and adaptation mechanisms using reinforcement learning, allowing the intelligent-based system to evolve and adapt to new types of cyber threats over time. Regular updates to the AI models ensure that the system remains capable of detecting emerging threats.

Evaluation and Validation

Field Testing

Deploy the intelligent-based system in a real-world power grid environment to validate its performance under actual operating conditions. This phase involves live monitoring and detection of potential cyber threats in the field.

Validation Metrics

Evaluate the system based on its detection rate, response efficiency, reduction in cyber attackincidents, and impact on the reliability and stability of the power system.

User Feedback

Gather feedback from system operators on the usability and effectiveness of the intelligent-based system. This feedback is used to make further improvements.

Documentation and Reporting

Results Documentation

Document the results of the simulations, field tests, and evaluations, highlighting the effectiveness of the intelligent-based system in improving cyber security in power systems and substation automation.

Recommendations for Implementation

Provide guidelines and recommendations for utilities and system operators on how to implement and maintain intelligent-based cyber security systems within their existing infrastructure.

By following this methodology, the research aims to achieve a robust cyber security solution that leverages intelligent-based systems to protect power systems and substation automation from evolving cyber threats.

To characterize and establish the causes of failure in cyber security in power systems and substation automation

Below is a table outlining the causes of failure in cyber security in power systems and substation automation, along with estimated percentages based on common industry analyses:

Table 1: Characterized and established causes of failure in cyber security in power systems and substation automation

Cause of Failure	Description	Percentage (%)
Lack of Adequate Security Measures	Insufficient firewalls, encryption, and intrusion detection systems to safeguard critical infrastructure.	25%
Human Error	Mistakes made by employees, such as poor password management, phishing susceptibility, or misconfigurations.	20%
Outdated Software and Hardware	Use of legacy systems and devices with outdated firmware or software that are vulnerable to cyber attacks.	15%
Insufficient Training and Awareness	Lack of proper training for operators and personnel to detect and respond to cyber threats effectively.	10%
Insider Threats	Malicious activities by individuals with access to the network, whether intentional or due to coercion.	10%
Weak Access Control Mechanisms	Poor implementation of access control policies, such as allowing unauthorized access to critical systems.	8%
Inadequate Network Segmentation	Lack of proper segmentation between operational and administrative networks, making it easier for attacks to spread.	7%
Failure to Patch Vulnerabilities	Failure to apply security patches to address known vulnerabilities in software, devices, or protocols.	5%
Complexity of the System	Complexity in managing the multiple interconnected devices and subsystems, leading to vulnerabilities in integration.	5%
Third-Party Vendor Risks	External contractors or third-party vendors introducing vulnerabilities or not adhering to security standards.	3%
Denial of Service (DoS) Vulnerabilities	Inability to mitigate or respond quickly to denial-of-service attacks, which can disable critical systems.	2%

The percentages represent estimates based on general industry observations and could vary depending on specific power system environments and their level of cyber security preparedness.

Note: These percentages are estimates and may vary depending on specific industry data and research findings.

Upload an image

This prompt requires an image that you need to add. Tap the image button to upload an image.

To design a SIMULINK model for cyber security in power systems and substation automation

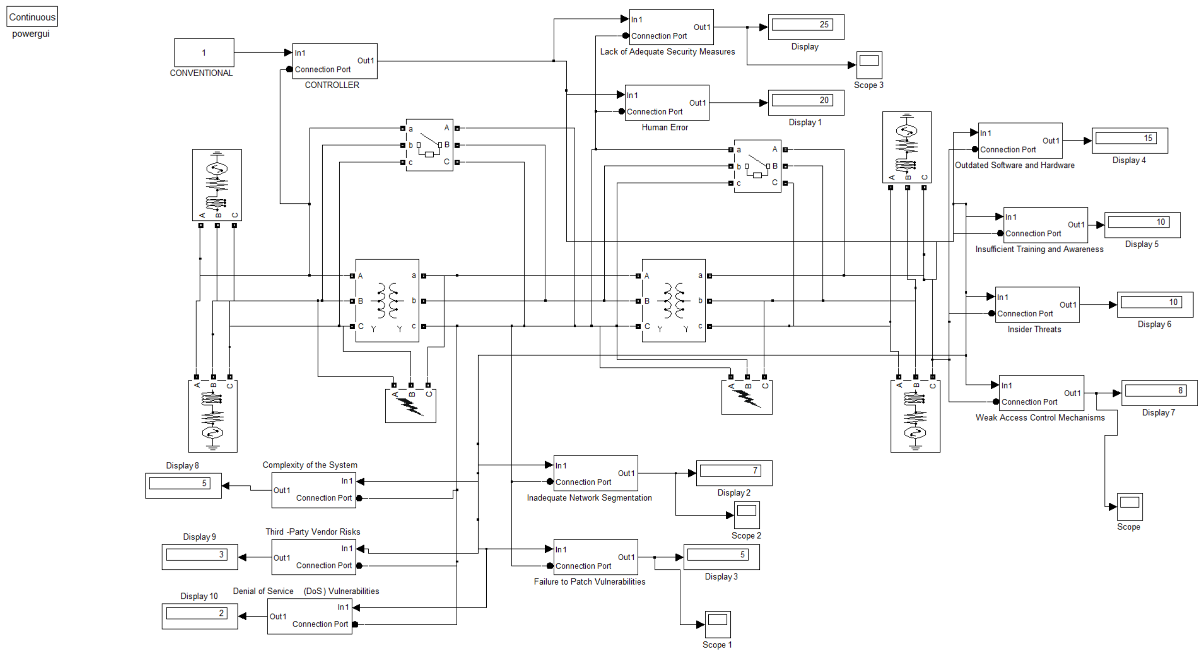
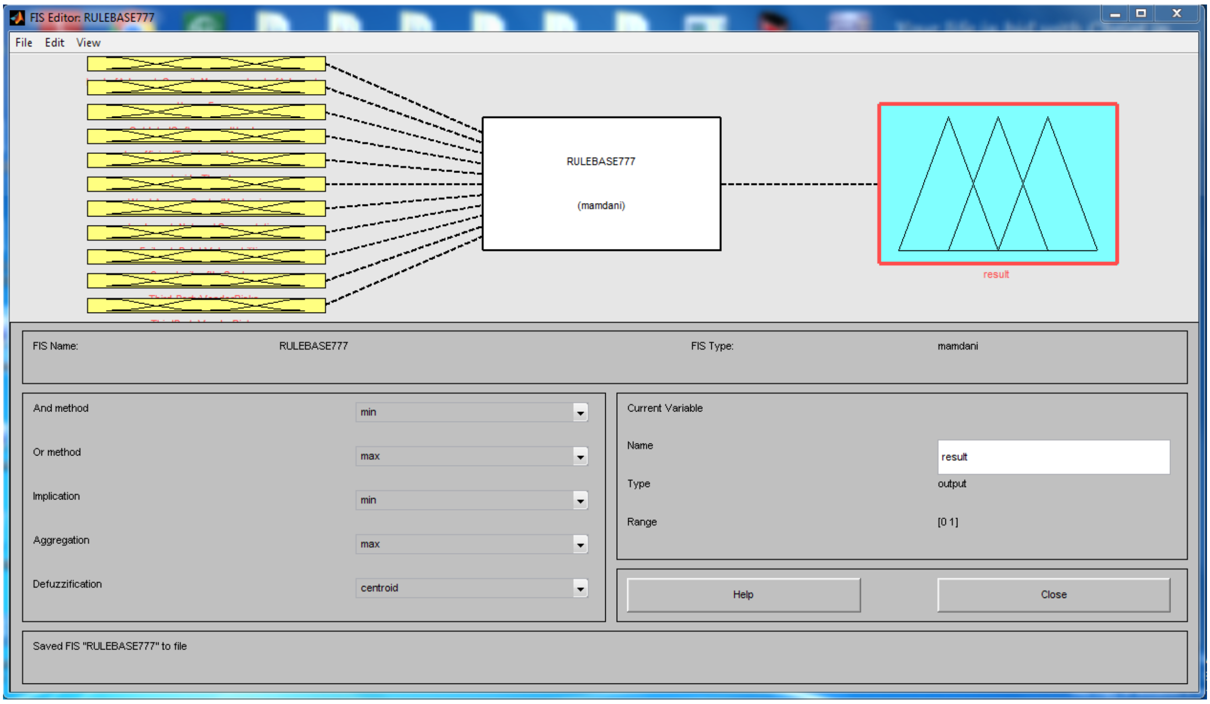

Continuous
powergui
1
CONVENTIONAL
In1
Out1
Connection Port
CONTROLLER
Lack of Adequate Security Measures
25
Display
Scope 3
Human Error
20
Display 1
Outdated Software and Hardware
15
Display 4
Insufficient Training and Awareness
10
Display 5
Insider Threats
10
Display 6
Weak Access Control Mechanisms
8
Display 7
Scope
Display 8
5
Complexity of the System
Inadequate Network Segmentation
7
Display 2
Scope 2
Display 9
3
Third -Party Vendor Risks
Failure to Patch Vulnerabilities
5
Display 3
Display 10
2
Denial of Service (DoS) Vulnerabilities
Scope 1

Figure 1: Designed SIMULINK model for cyber security in power systems and substation automation



FIS Name: RULEBASE777

FIS Type: mamdani

And method: min

Or method: max

Implication: min

Aggregation: max

Defuzzification: centroid

Current Variable

Name: result

Type: output

Range: [0 1]

Saved FIS "RULEBASE777" to file

Figure 2: Designed fuzzy inference system((FIS) that will reduce the causes of failure in cyber security in power systems and substation automation

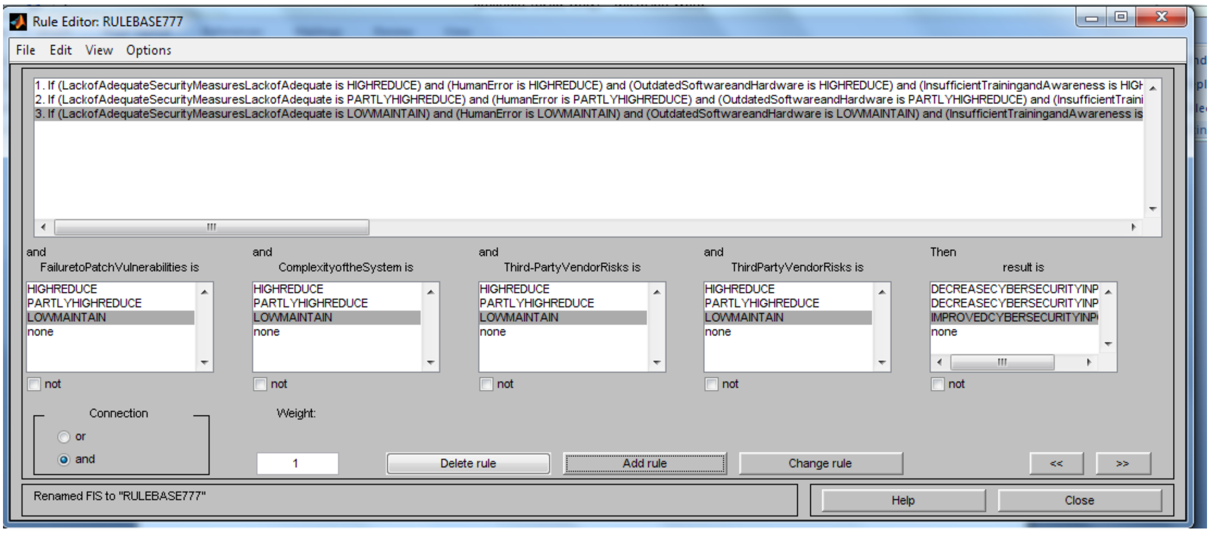
The results obtained are as shown in figures 8 through 11

To design a rule base that will reduce the causes of failure in cyber security in power systems and substation automation

This has eleven inputs of Lack of Adequate Security Measures, Human Error, Outdated Software and Hardware,Insufficient Training and Awareness, Insider Threats, Weak Access Control Mechanisms, Inadequate Network Segmentation, Failure to Patch Vulnerabilities,Complexity of the System, Third-Party Vendor Risks and Denial of Service (DoS) Vulnerabilities. It also has an output of result.

This has three stipulated rules that were comprehensively detailed in table 2

To train ANN in the rule base for effective reduction of CAUSES OF FAILURE in cyber security in power systems and substation automation



Rule Editor: RULEBASE777

1. If (LackofAdequateSecurityMeasuresLackofAdequate is HIGHREDUCE) and (HumanError is HIGHREDUCE) and (OutdatedSoftwareandHardware is HIGHREDUCE) and (InsufficientTrainingandAwareness is HIGH
2. If (LackofAdequateSecurityMeasuresLackofAdequate is PARTLYHIGHREDUCE) and (HumanError is PARTLYHIGHREDUCE) and (OutdatedSoftwareandHardware is PARTLYHIGHREDUCE) and (InsufficientTraini
3. If (LackofAdequateSecurityMeasuresLackofAdequate is LOWMAINTAIN) and (HumanError is LOWMAINTAIN) and (OutdatedSoftwareandHardware is LOWMAINTAIN) and (InsufficientTrainingandAwareness is

and FailuretoPatchVulnerabilities is	and ComplexityoftheSystem is	and Third-PartyVendorRisks is	and ThirdPartyVendorRisks is	Then result is
HIGHREDUCE	HIGHREDUCE	HIGHREDUCE	HIGHREDUCE	DECREASECYBERSECURITYINP
PARTLYHIGHREDUCE	PARTLYHIGHREDUCE	PARTLYHIGHREDUCE	PARTLYHIGHREDUCE	DECREASECYBERSECURITYINP
LOWMAINTAIN	LOWMAINTAIN	LOWMAINTAIN	LOWMAINTAIN	IMPROVEDCYBERSECURITYINP
none	none	none	none	none
□ not	□ not	□ not	□ not	□ not

Connection: ○ or ● and

Weight: 1

Renamed FIS to "RULEBASE777"

Figure 3: Designed rule base that will reduce the causes of failure in cyber security in power systems and substation automation

Table 2: Comprehensively detailed designed rule base that will reduce the causes of failure in cyber security in power systems and substation automation

IF Lack of Adequate Security Measures IS LOW MAINTAIN	IF Lack of Adequate Security Measures IS PARTLY HIGH REDUCE	IF Lack of Adequate Security Measures IS HIGH REDUCE
AND Human Error IS LOW MAINTAIN	AND Human Error IS PARTLY HIGH REDUCE	AND Human Error IS HIGH REDUCE
AND Outdated Software and Hardware IS LOW MAINTAIN	AND Outdated Software and Hardware IS PARTLY HIGH REDUCE	AND Outdated Software and Hardware IS HIGH REDUCE
AND Insufficient Training and Awareness IS LOW MAINTAIN	AND Insufficient Training and Awareness IS PARTLY HIGH REDUCE	AND Insufficient Training and Awareness IS HIGH REDUCE
AND Insider Threats IS LOW MAINTAIN	AND Insider Threats IS PARTLY HIGH REDUCE	AND Insider Threats IS HIGH REDUCE
AND Weak Access Control Mechanisms IS LOW MAINTAIN	AND Weak Access Control Mechanisms IS PARTLY HIGH REDUCE	AND Weak Access Control Mechanisms IS HIGH REDUCE
AND Inadequate Network Segmentation IS LOW MAINTAIN	AND Inadequate Network Segmentation IS PARTLY HIGH REDUCE	AND Inadequate Network Segmentation IS HIGH REDUCE
AND Failure to Patch Vulnerabilities IS LOW MAINTAIN	AND Failure to Patch Vulnerabilities IS PARTLY HIGH REDUCE	AND Failure to Patch Vulnerabilities IS HIGH REDUCE
AND Complexity of the System IS LOW MAINTAIN	AND Complexity of the System IS PARTLY HIGH REDUCE	AND Complexity of the System IS HIGH REDUCE
AND Third-Party Vendor Risks IS LOW MAINTAIN	AND Third-Party Vendor Risks ISPARTLY HIGH REDUCE	AND Third-Party Vendor Risks IS HIGH REDUCE
AND Denial of Service (dos) Vulnerabilities IS LOW MAINTAIN	Anddenial of Service (dos) Vulnerabilities IS PARTLY HIGH REDUCE	AND Denial of Service (dos) Vulnerabilities IS HIGH REDUCE
Then result is improved in cyber security in power	Then result is decrease in cyber security in power	Then result is decrease in cyber security in power

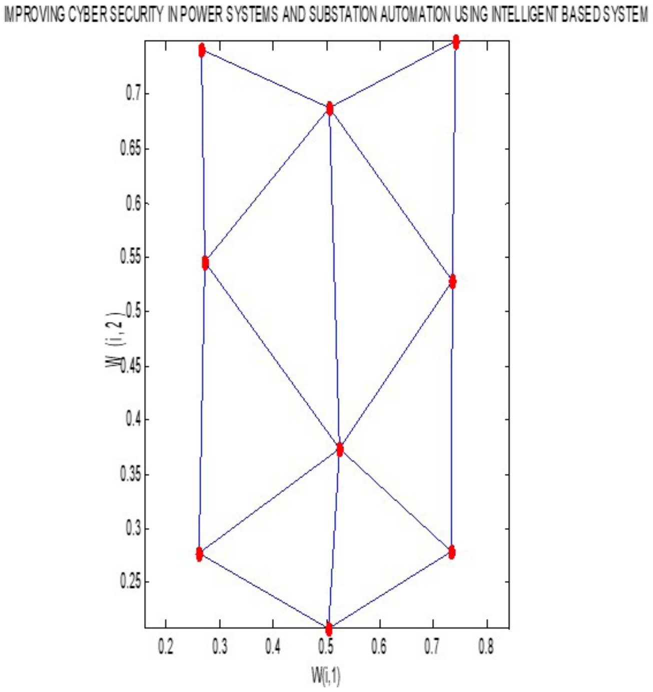


Figure 4: Trained ANN rule base for effective reduction of causes of failure in cyber security in power systems and substation automation

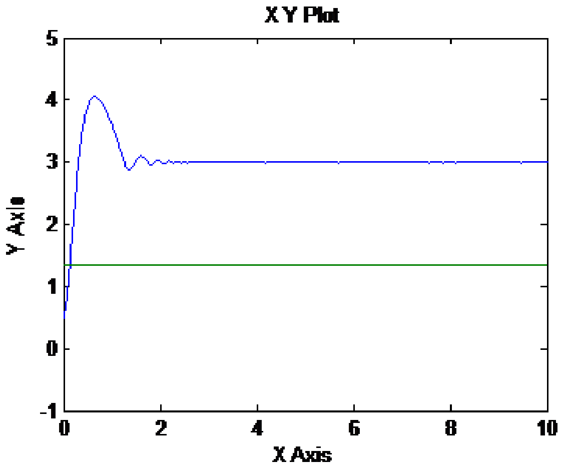


Figure 5: Number of ANN training in rule base for effective reduction of CAUSES OF FAILURE in cyber security in power systems and substation automation

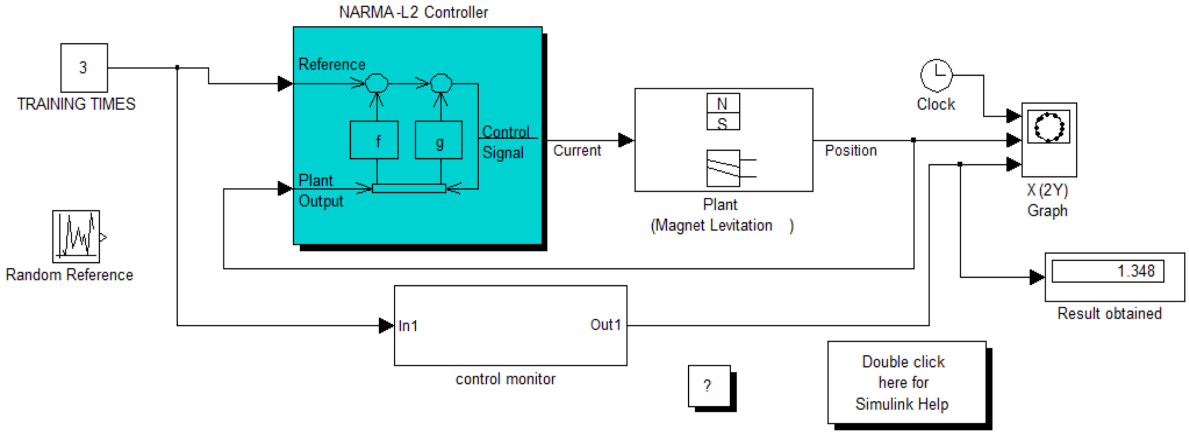


Figure 6: Result obtained during training ANN in the rules

To develop an algorithm for the process

1. Characterize and establish the causes of failure in cyber security in power systems and substation automation
2. Identify Lack of Adequate Security Measures
3. Identify Human Error
4. Identify Outdated Software and Hardware
5. Identify Insufficient Training and Awareness
6. Identify Insider Threats
7. Identify Weak Access Control Mechanisms
8. Identify Inadequate Network Segmentation
9. Identify Failure to Patch Vulnerabilities
10. Identify Complexity of the System
11. Identify Third-Party Vendor Risks
12. Identify Denial of Service (DoS) Vulnerabilities
13. Design a SIMULINK model for cyber security in power systems and substation automation integrate 2 through 12
14. Design a rule base that will reduce the causes of failure in cyber security in power systems and substation automation
15. Train ANN in the rule base for effective reduction of CAUSES OF FAILURE in cyber security in power systems and substation automation
16. Integrate 14 and 15
17. Integrate 16 in 13
18. Do the causes of FAILURE in cyber security in power systems and substation automation reduce when 16 was integrated in 13?
19. IF NO go to 17
20. IF YES go to 21
21. Improved cyber security in power systems and substation automation
22. Stop
23. End

To design a SIMULINK model for improving cyber security in power systems and substation automation using intelligent based system

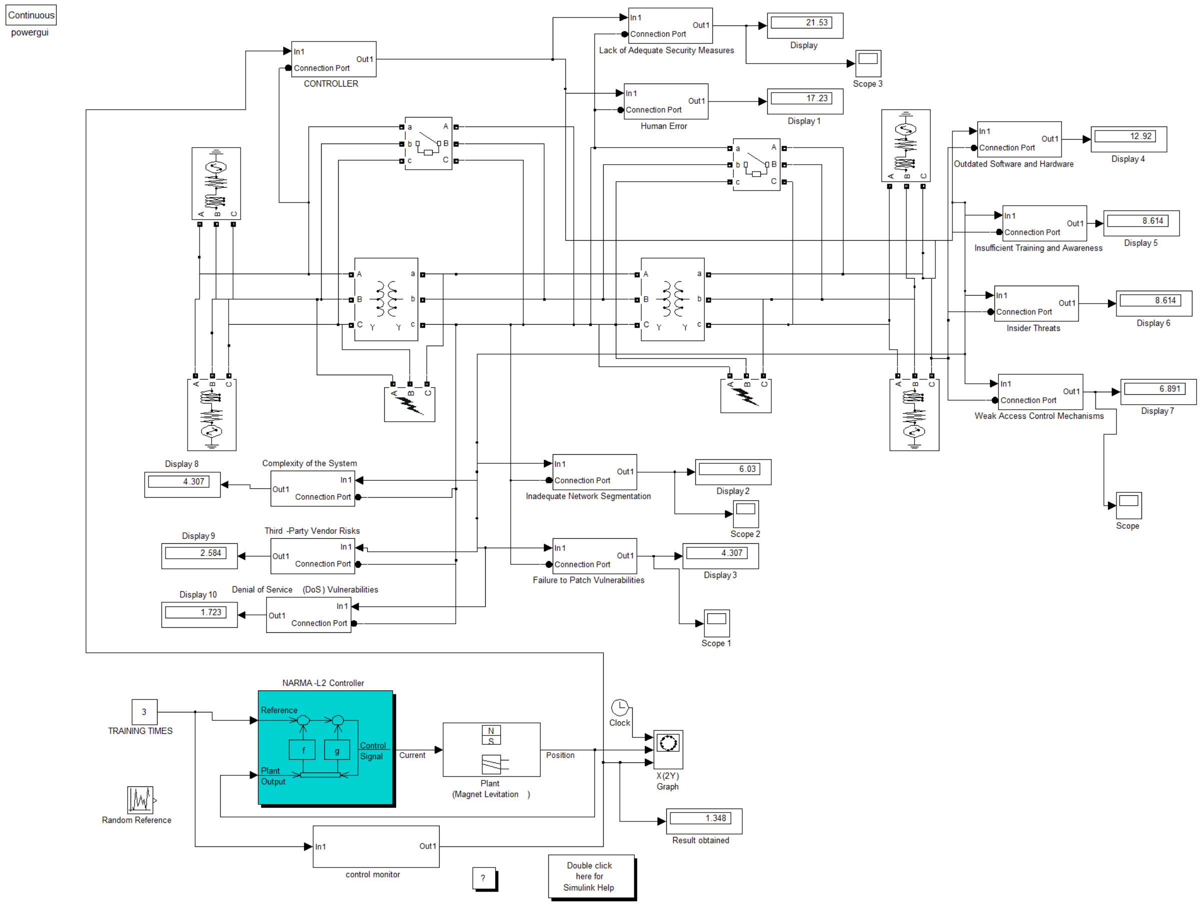


Figure 7: Designed SIMULINK model for improving cyber security in power systems and substation automation using intelligent based system

The results obtained are as shown in figures 8 through 11

To validate and justify the percentage of improvement in the reduction of causes of FAILURE in cyber security in power systems and substation automation

To find percentage improvement in the reduction of Lack of Adequate Security Measures that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system

Conventional Lack of Adequate Security Measures =25%

Intelligent based system Lack of Adequate Security Measures =21.53%

%improvement in the reduction of Lack of Adequate Security Measures that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=

Conventional Lack of Adequate Security Measures - Intelligent based system Lack of Adequate Security Measures

%improvement in the reduction of Lack of Adequate Security Measures that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=25% - 21.53%

%improvement in the reduction of Lack of Adequate Security Measures that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=3.47%

To find percentage improvement in the reduction of outdated software and hardwarethat causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system

Conventional outdated software and hardware =15%

Intelligent based system outdated software and hardware =12.92%

%improvement in the reduction of outdated software and hardware that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system= Conventional outdated software and hardware - Intelligent based system outdated software and hardware

%improvement in the reduction of outdated software and hardwareFAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=15% -12.92 %

%improvement in the reduction of outdated software and hardware that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=2.08%

To find percentage improvement in the reduction of Weak Access Control Mechanisms that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system

Conventional Weak Access Control Mechanisms =8%

Intelligent based system Weak Access Control Mechanisms =6.9%

%improvement in the reduction of Weak Access Control Mechanisms that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system= Conventional Weak Access Control Mechanisms - Intelligent based system Weak Access Control Mechanisms

%improvement in the reduction of Weak Access Control Mechanisms FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=8% - 6.9%

%improvement in the reduction of Weak Access Control Mechanisms that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=1.1%

To find percentage improvement in the reduction of Denial of Service (DoS) Vulnerabilities that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system

Conventional Denial of Service (DoS) Vulnerabilities =2%

Intelligent based system Denial of Service (DoS) Vulnerabilities =1.7%

%improvement in the reduction of Denial of Service (DoS) Vulnerabilities that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=

Conventional Denial of Service (DoS) Vulnerabilities - Intelligent based system Denial of Service (DoS) Vulnerabilities

%improvement in the reduction of Denial of Service (DoS) Vulnerabilities FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=2% - 1.7%

%improvement in the reduction of Denial of Service (DoS) Vulnerabilities that causes FAILURE in cyber security in power systems and substation automation when intelligent based system was incorporated in the system=0.3%

RESULTS AND DISCUSSION

Table 3: Comparison of conventional and Intelligent based system Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation using intelligent based system

Tome(s)	Conventional Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)	Intelligent based system Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)
1	25	21.53
2	25	21.53
3	25	21.53
4	25	21.53
10	25	21.53

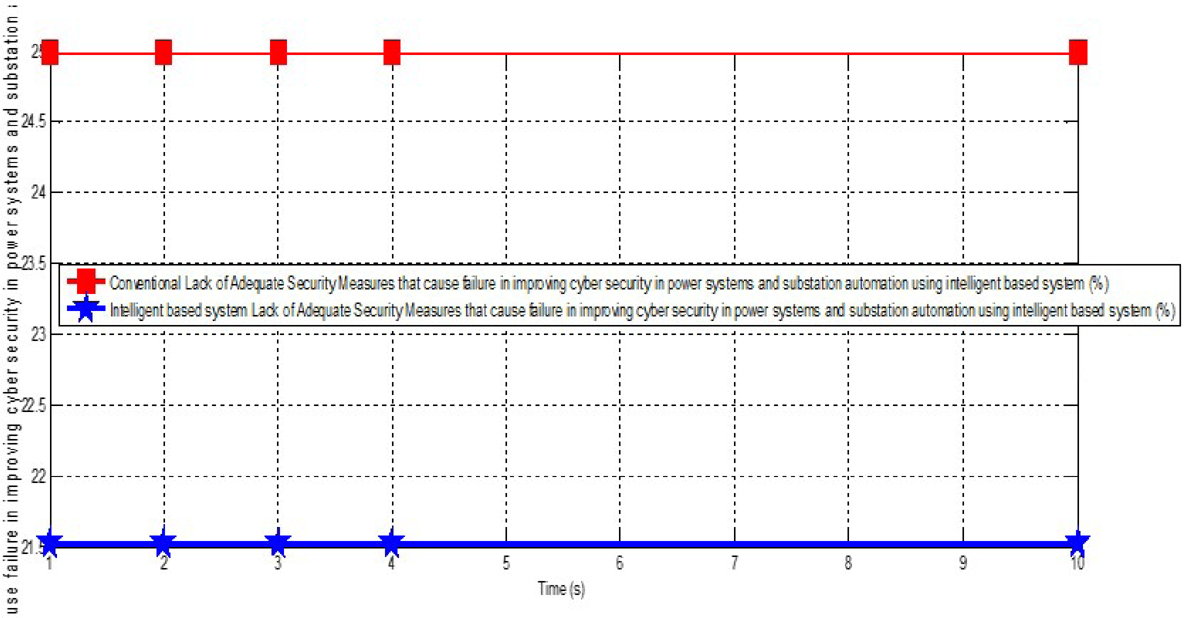


Figure 8: Comparison of conventional and Intelligent based system Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation using intelligent based system

The conventional Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation was25%. On the other hand, when an intelligent based system was incorporated into the system, it drastically reduce the cause failure in improving cyber security in power systems and substation automation to21.53%.

Table 4: Comparison of conventional and Intelligent based system outdated software and hardware that cause failure in improving cyber security in power systems and substation automation using intelligent based system

Tome(s)	Conventional outdated software and hardware that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)	Intelligent based system Lack of outdated software and hardware that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)
1	15	12.92
2	15	12.92
3	15	12.92
4	15	12.92
10	15	12.92

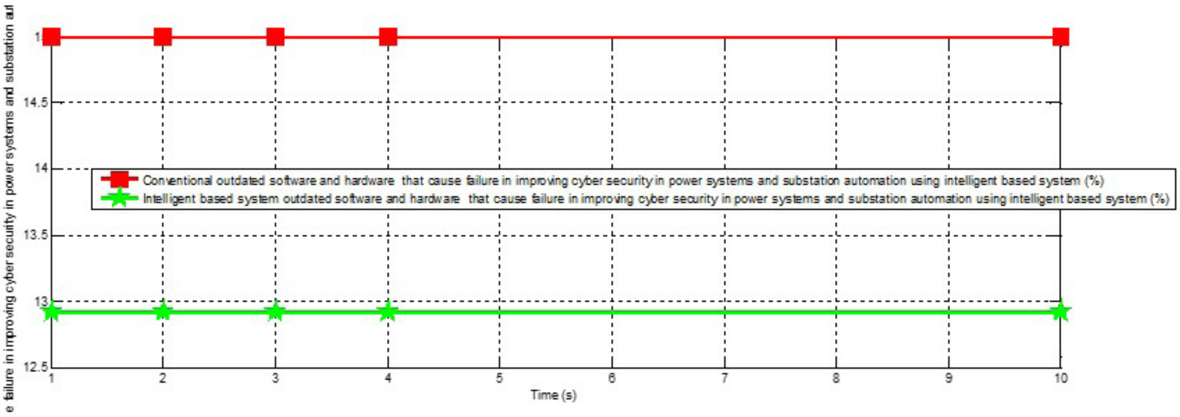


Figure 9: Comparison of conventional and Intelligent based system outdated software and hardware that cause failure in improving cyber security in power systems and substation automation using intelligent based system

The conventional outdated software and hardware that cause failure in improving cyber security in power systems and substation automation was 15%. Meanwhile, when an intelligent based system was inculcated in the system, it became reduced to12.92% thereby enhancing the performance of cyber security in power systems and substation automation by 2.08%.

Table 5: Comparison of conventional and Intelligent based system Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation using intelligent based system

Tome(s)	Conventional Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)	Intelligent based system Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)
1	8	6.9
2	8	6.9
3	8	6.9
4	8	6.9
10	8	6.9

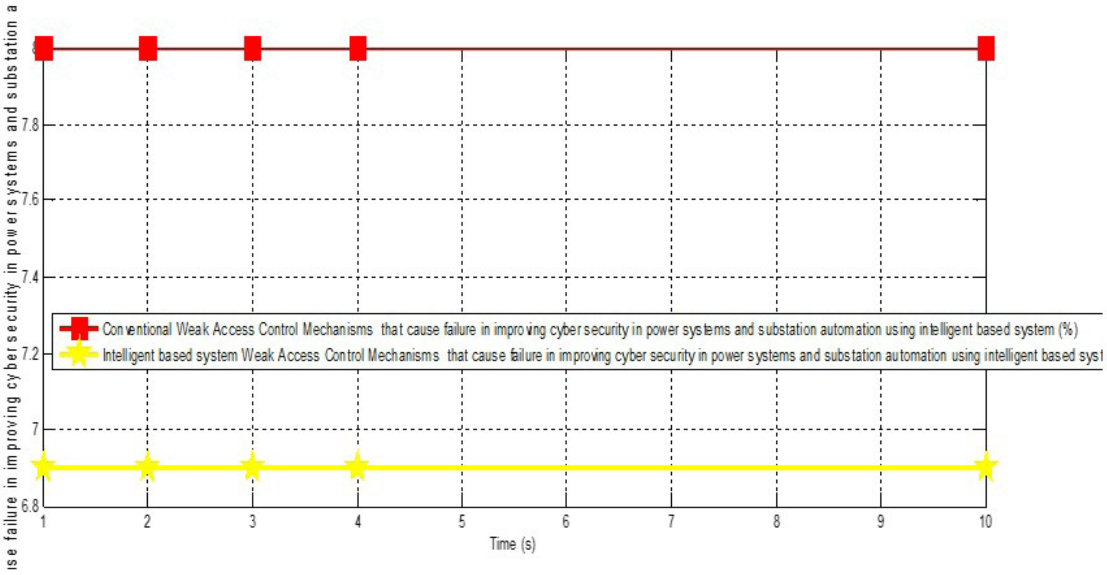


Figure 10: Comparison of conventional and Intelligent based system Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation using intelligent based system

The conventional Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation was 8%. However, when an intelligent based system was integrated in the system, it was reduced to 6.9%.

Table 6: Comparison of conventional and Intelligent based system Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation using intelligent based system

Tome(s)	Conventional Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)	Intelligent based system Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation using intelligent based system (%)
1	2	1.7
2	2	1.7
3	2	1.7
4	2	1.7
10	2	1.7

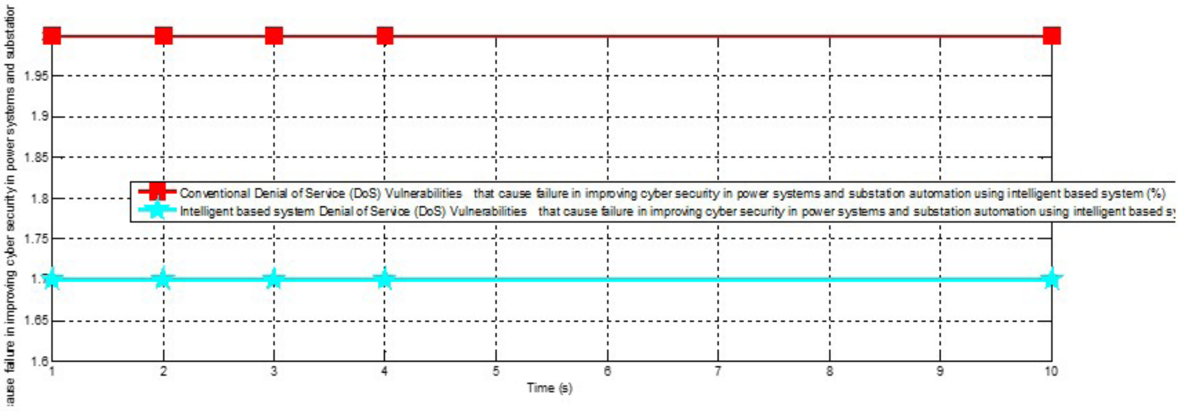


Figure 11: Comparison of conventional and Intelligent based system Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation using intelligent based system

The conventional Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation was 2% while when an intelligent based system was incorporated in the system, it automatically reduced to1.7%. Finally, with these results obtained, It vehemently shows that the percentage improvement in cyber security in power systems and substation automation was 0.3%.

CONCLUSION

The persistent failure in cyber security in power systems and substation automation that has dwindled business activities in the country are caused by Lack of Adequate Security Measures, Human Error, Outdated Software and Hardware, Insufficient Training and Awareness, Insider Threats, Weak Access Control Mechanisms, Inadequate Network Segmentation, Failure to Patch Vulnerabilities, Complexity of the System, Third-Party Vendor Risks and Denial of Service (DoS) Vulnerabilities. This is surmounted by introducing improving cyber security in power systems and substation automation using intelligent based system. To achieve this, it is done in this procedure characterizing and establishing the causes of failure in cyber security in power systems and substation automation, designing a SIMULINK model for cyber security in power systems and substation automation, designing a rule base that will reduce the causes of failure in cyber security in power systems and substation automation,training ANN in the rule base for effective reduction of causes of failure in cyber security in power systems and substation automation, developing an algorithm for the process, designing a SIMULINK model for improving cyber security in power systems and substation automation using intelligent based system and validating and justifying the percentage of improvement in the reduction of causes of failure in cyber security in power systems and substation automation. The results obtained were the conventional Lack of Adequate Security Measures that cause failure in improving cyber security in power systems and substation automation was25%. On the other hand, when an intelligent based system was incorporated into the system, it drastically reduce the cause failure in improving cyber security in power systems and substation automation to21.53%, the conventional outdated software and hardware that cause failure in improving cyber security in power systems and substation automation was 15%. Meanwhile, when an intelligent based system was inculcated in the system, it became reduced to12.92% thereby enhancing the performance of cyber security in power systems and substation automation by 2.08%, the conventional Weak Access Control Mechanisms that cause failure in improving cyber security in power systems and substation automation was 8%. However, when an intelligent based system was integrated in the system, it was reduced to 6.9% and the conventional Denial of Service (DoS) Vulnerabilities that cause failure in improving cyber security in power systems and substation automation was 2% while when an intelligent based system was incorporated in the system, it automatically reduced to1.7%. Finally, with these results obtained, It vehemently shows that the percentage improvement in cyber security in power systems and substation automation was 0.3%..

Contribution to Knowledge

The application of intelligent-based systems to enhance cyber security in power systems and substation automation can contribute to knowledge in several ways:

Advanced Anomaly Detection

The development of novel anomaly detection algorithms that can accurately identify cyber threats in real-time, even in the presence of noise and adversarial attacks, can significantly improve the detection capabilities of existing security systems.

Automated Threat Analysis

The use of machine learning techniques to automate the analysis of large volumes of network traffic can help identify patterns indicative of malicious activity that may be difficult to detect manually.

Enhanced Data Integrity

The integration of block chain technology can provide tamper-proof records of system events, ensuring data integrity and increasing trust in the system.

Privacy-Preserving Data Analysis

The development of privacy-preserving data mining techniques can enable the analysis of data without compromising sensitive information, allowing for the development of more effective security measures while protecting user privacy.

Evaluation of Intelligent-Based Security Solutions

The evaluation of different intelligent-based security solutions in real-world power system environments can provide valuable insights into their effectiveness and identify areas for improvement.

By addressing these research gaps, this work can contribute to the following areas of knowledge:

Cyber Security in Critical Infrastructure

This research can provide valuable insights into the application of intelligent-based systems to enhance the security of critical infrastructure, such as power systems.

Machine Learning and Cyber Security

This work can advance the application of machine learning techniques to cyber security problems, particularly in complex and heterogeneous environments.

Block Chain Technology in Cyber Security

This research can explore the potential of block chain technology to improve data integrity and security in power systems.

Privacy-Preserving Data Analytics

This work can contribute to the development of new methods for analyzing data while protecting sensitive information.

Intelligent Systems for Cyber Security

This research can advance the understanding of how intelligent systems can be used to address cyber security challenges in a variety of domains.

Overall, this research can contribute to the development of more effective and resilient cyber security solutions for power systems and substation automation, ensuring the reliability and security of critical infrastructure.

REFERENCES

Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. In *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCSW)* (pp. 495–500). IEEE.

Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., & Poolla, K. (2013). Smart grid data integrity attacks: Characterizations and countermeasures. *IEEE Transactions on Smart Grid, 4*(3), 1244–1253.

Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid, 4*(2), 847–855.

Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security, 14*(1), Article 13.

Mackiewicz, R. E. (2006). Overview of IEC 61850 and benefits. *IEEE Transactions on Power Delivery, 21*(1), 23–30.

Mousavian, S. H., & Masoum, M. A. S. (2018). A review of cyber-physical security of smart grid infrastructure. *IEEE Transactions on Industrial Informatics, 14*(6), 2236–2244.

Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Cyber-physical attacks in power networks: Models, fundamental limitations, and monitor design. *IEEE Transactions on Automatic Control, 58*(11), 2715–2729.

Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE, 100*(1), 210–224.

Wei, J., Wu, W., & Sun, Y. (2017). Hybrid intrusion detection for substation automation system based on deep learning and expert rules. *IEEE Transactions on Power Delivery, 32*(2), 810–818.

Zhang, M., Gao, Y., & Li, X. (2016). Artificial intelligence applications in smart grid: A survey. *IEEE Transactions on Industrial Informatics, 12*(3), 801–808.