ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

CYBER-RESILIENT NETWORK ARCHITECTURE FOR SMART GRID

Azhar Ashraf

Assistant Professor Chandigarh University, Mohali, Punjab

Shishir Singh

Computer Science and Engineering Chandigarh University, Mohali, Punjab

Devesh Kumar Upadhyay

Computer Science and Engineering Chandigarh University, Mohali, Punjab

Shruti Sharma

Computer Science and Engineering Chandigarh University, Mohali, Punjab

Somil Bisht

Computer Science and Engineering Chandigarh University, Mohali, Punjab

Nimmanagoti Anil

Computer Science and Engineering Chandigarh University, Mohali, Punjab

ABSTRACT—

For smart grids dealing with changing cyber threats, guaranteeing a cyber-resilient network is important. This project uses artificial intelligence, specifically Convolutional Neural Networks (CNN), to improve grid security by detecting and mitigating phishing, malware, and DDoS threats. The system correctly detects phishing 33.1% of the time, malware 31.4% of the time, and DDoS attacks 32.4% of the time, with low false positive rates of 0.7% for phishing, 1.0% for malware, and 1.4% for DDoS.

To precisely spot all unusual login behaviours, the system thoroughly integrates real-time threat intelligence, in-depth behavioural analysis, and immediate proactive alerts, ultimately achieving a 90% accuracy rate. User feedback confirms its effectiveness and usability through a satisfaction rate of 92% and an adoption rate of 78%. The system secures all communications through encryption, two-factor authentication, and identity verification, fully complying with GDPR and NIST SP 800-63B. This AI framework both strengthens how secure the grid is and keeps operations strong by always adjusting to new dangers.

Keywords: cybersecurity automation in power systems, secure grid communication, AI-powered security, smart grid security compliance, and machine learning for cybersecurity; Adaptive security architecture; proactive cyber defence; intrusion detection and prevention; threat intelligence in energy networks; and cyber- resilient smart grids.

I. INTRODUCTION

The thorough combination of digital technologies in every modern smart grid has considerably improved energy infrastructure's efficiency as well as its reliability. Still, this digital change has introduced several cybersecurity dangers; these dangers include many advanced social engineering attacks, multiple phishing scams, several malware threats, and many Distributed Denial-of-Service (DDoS) attacks that target important energy networks[1]. These cyber-threats pose severe risks to grid stability, data integrity, and operational resilience, making cybersecurity a top priority for smart grid systems [3][4].

Firewalls and access restrictions are among the conventional cybersecurity tools that mostly rely on static defences, which find it difficult to respond to fast-changing threats, especially against social engineering techniques, malware intrusion, and massive DDoS attacks.

Considering the growing complexity of cyberattacks, one must move toward cyber resilience. This technique goes beyond standard security by including real-time threat detection, automated response, network redundancy, and self-healing capabilities in the grid design. This paper proposes a Cyber- robust Network Architecture for Smart Grids that combines AI- driven cybersecurity methodologies with strong network architecture to prevent phishing, malware, social engineering, and DDoS assaults. Examining network activity, emails, and conversation patterns using machine learning methods, the system finds malevolent intent before an attack may compromise the grid. Natural language processing and anomaly-based detection enable the AI system to spot dubious communication patterns, false identities, malware signatures, unusual traffic spikes suggestive of DDoS attacks, and deceptive strategies used to access energy networks. The network architecture incorporates redundant communication lines, intrusion-tolerant distributed control systems, and zero-trust security models to ensure uninterrupted operations in the case of an attack

The system includes an AI-powered threat detection module that evaluates incoming messages, email attachments, and executable files for potential phishing and malware threats. This module examines phishing keywords, communication styles, viral patterns, and sender behavior. The system checks URLs for validity to prevent phishing websites impersonating reputable platforms.

Behavioral analysis prevents social engineering and malware attacks by detecting unusual user activity, such as attempts to lure employees into providing sensitive information or running harmful software.

The suggested architecture prioritizes self-healing capabilities, enabling automated incident response systems to swiftly detect, isolate, and eliminate threats.When phishing, malware, or DDoS attacks are detected, the system automatically warns administrators, quarantines malicious files and communications, disables compromised accounts, and isolates network segments.

To protect against DDoS attacks, the system uses traffic filtering, rate limitation, and anomaly-based analysis to minimize disruptions and maintain service uptime. The architecture utilizes software-defined networking for dynamic traffic rerouting and blockchain technology for secure data integrity, resulting in reliable grid operations.

This technology makes smart grids more resilient to attacks by automating threat mitigation, implementing adaptive security frameworks, and providing redundant communication channels. The suggested AI-powered cybersecurity architecture provides protection against phishing, malware, and DDoS attacks while also providing grid resilience, operational continuity, and data security. The technology provides energy firms and grid operators with cyber risk management tools such as machine learning, natural language processing, and real-time threat data. This solution increases smart grid cybersecurity by providing adaptive defense against emerging threats, ensuring future energy infrastructure security.

Current smart grid cybersecurity solutions cannot keep up with emerging threats like malware, DDoS, and phishing due to their reliance on fixed defenses. This innovation bridges the cybersecurity gap with an AI-powered system that detects threats in real-time, responds automatically, and heals itself. Our system uses machine learning, including NLP and CNNs, to detect and mitigate cyber threats. Our system combines AI-powered defense with robust network architecture to maintain operational continuity and data integrity during ongoing attacks.

II. LITERATURE REVIEW

The rising digitization of smart grids has brought new cybersecurity concerns, notably in fighting advanced cyber threats including phishing, malware, Distributed Denial-of- Service (DDoS) assaults, and social engineering strategies. Traditional security solutions, including firewalls and rule- based intrusion detection systems, cannot keep up with increasing attack techniques [1]. Researchers emphasize the necessity of cyber resistance structure that integrates AI contrast Safety of adaptive network protection mechanisms [2].

AI-Based Threat Detection for Smart Grids

Detection of threats based on artificial intelligence of intellectual network AI plays an important role in increasing smart cyber security. Machine learning model is used for monitoring. Network traffic pattern, irregular detection and prevention Enjoy the activities as a violation of the operation. CNNs and RNNs boost IDS accuracy for recognizing malware and DDoS assaults in energy networks [7].

NLP improves phishing detection by assessing email content, identifying bogus communication patterns, and preventing unauthorized access to vital grid control systems.

AI-powered threat intelligence tools discover, analyze, and mitigate cyber threats in real-time, minimizing false positives in anomaly detection systems [8]. Jain and Gupta's (2017) study of machine learning-based phishing detection techniques reveals its utility in averting cyber assaults[5].

Resilient Network Architectures for Smart Grids

To be truly cyber-resilient, a network design should have proactive security techniques to guarantee operational continuity during assaults, in addition to AI-powered detection. SDN dynamically reroutes traffic and separates essential grid pieces to avoid cascade failures [6]. Blockchain technology promotes data integrity and security in smart grids by banning unauthorized alterations to vital infrastructure data.

Zero-trust security approaches rely on ongoing authentication and access limits to avoid insider attacks and unwanted access. Self-healing distributed control systems help smart grids detect, contain, and recover from cyber-attacks with little downtime [9].

Cyber Resilience for Energy Networks

Adaptive security frameworks are vital for managing growing threats, according to studies. AI-powered incident response systems identify hazardous behaviors, block unauthorized access, and assure service availability during cyber assaults. Compliance with security standards, including GDPR and NIST SP 800- 53[12], as well as advise from Akamai Technologies and Gartner [11], increases the regulatory framework for safeguarding energy networks from cyber threats.

Research Gaps and Future Directions

Recent breakthroughs in AI-powered security solutions, strong network topologies, and automated threat mitigation tactics provide a solid framework for establishing cyber resilience in smart grids.

III METHODOLOGY

A Research Design

This research employs a mixed-methods strategy for cyber- resilience, using qualitative and quantitative methods to design, develop, and implement an AI-based smart grid network. The system will be further implemented, deployed, and tested in a realistic energy network environment to assess its effectiveness with respect to detection and mitigation of phishing, malware, Distributed Denial-of-Service (DDoS) attacks and social engineering approaches while also maintaining grid stability and operational continuity [10].

B Data Collection

Primary Data: Operational Data from Smart Grid: Real-time data will be gathered from SCADA and IoT-enabled energy meters, as well as communication networks for the grid, to evaluate cyber-resilience under attack scenarios.

The system will monitor and collect data on the user's interaction to measure the usefulnessness, effectiveness and usability of the AI-driven security system.

Network Anomaly Detection: Illegitimate access attempts, traffic anomalies, or behavioral aberrations that imply phishing, malware intrusion, or DDoS attacks will be detected by the system in real time.

Secondary Data:

Cyber Threat Datasets: AI models will be trained on publicly available datasets of phishing, malware, and DDoS attacks (such as PhishTank, OpenPhish, VirusTotal, and DDoS intelligence platforms)

Energy Sector Cybersecurity Reports: NIST, DOE, and ENISA security frameworks and attack patterns will be used to inform the system's adaptive threat models.

C System Development

The proposed system will incorporate the following key components:

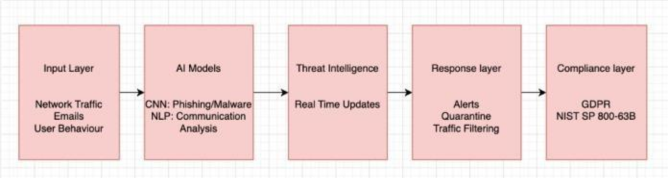

Fig 1: Architecture of the AI-driven cybersecurity framework, integrating real-time threat detection, behavioural analysis, and compliance measures for smart grids.

Phishing and Malware Detection Model: This model employs predictive analytics to scan emails, file attachments and metadata for phishing attempts and malware threats capable of affecting smart grid communication networks. The system will prevent cyber enemies from entering into critical infrastructure by identifying textual, structural, and behavioural abnormalities.

AI-Powered Behavioral Analyzer: The system monitors user activities, such as log in at odd hours, engagement with phishing emails, executing suspicious files and transferring huge datasets, using AI. It can help to detect malware infections, social engineering exploitation attempts, and account compromises.

DDoS Mitigation Engine: The system must analyse traffic patterns in real-time to detect volumetric spikes, abnormal request behaviours, and botnet-driven acts typically hinting to a DDoS attack on smart grid communication networks. Grid stability and availability will be ensured using advanced mitigation mechanisms, including rate limiting, anomaly-based filtering, and real-time threat intelligence.

Propose a real-time danger warning system: In this method, users of energy system and grid operator is warned. You may take quick response, Potential Cyber-AKS.

Securing the critical infrastructure. Protect against phishing. And automated tasks like a malware attack, URL.

Isolation and access lock, e-mail and avatar will be restricted. In case of DDOS Attack, Distributed preventive mechanisms such as traffic filtering or download balancing is used. In each case, judicial inquiry was held, and a continuous lessons- learned loop on improving future threat identification and response capabilities was created.

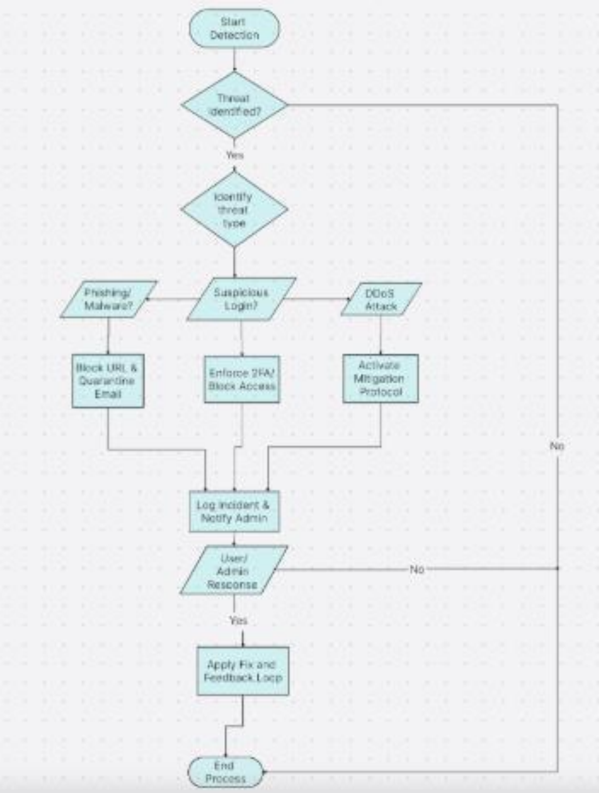

Fig 2: Real-Time Threat Alert System

D Security Framework and Compliance Measures:

This system complies with the following international security standards: GDPR and NIST SP 800-63B, protect user data Integrity of communication to build safe and cyber resistance net. Many defensive layers are included in safety. Architecture to increase protection of cyber ships:

Numerous defence layers are incorporated into the security architecture to increase protection against cyber threats:

Encryption Mechanism: Prevent undesirable access Communication and confidential data are encrypted in the industry. Standard encryption algorithm.

Two Characteristic Certification: Improves the identity of 2FA request a few types of users proof.

Personality confirmation: Continuous authentication measures Make sure only true users can access the system. Therefore, it prevents illegal infringement.

Adaptive Threat Intelligence: The powered AI system is always learning from new cyber threats, allowing it to dynamically adjust defence measures.

Adaptive intelligence threat: AI system Research on the new cybersis dynamically, allow you to dynamically Accurate protection measures.

Real -time invasion detection: Login is actively controlled trying, user activity and network detection potential safety disorder

Compliance with Rules: Guaranteed GDPR data Protection principles and safety requirements NIST. Therefore, there was a compliance with regulatory requirements to.

By combining these safety measures, Identify and soften the cyber waterfall, but the term operation stability and data protection.

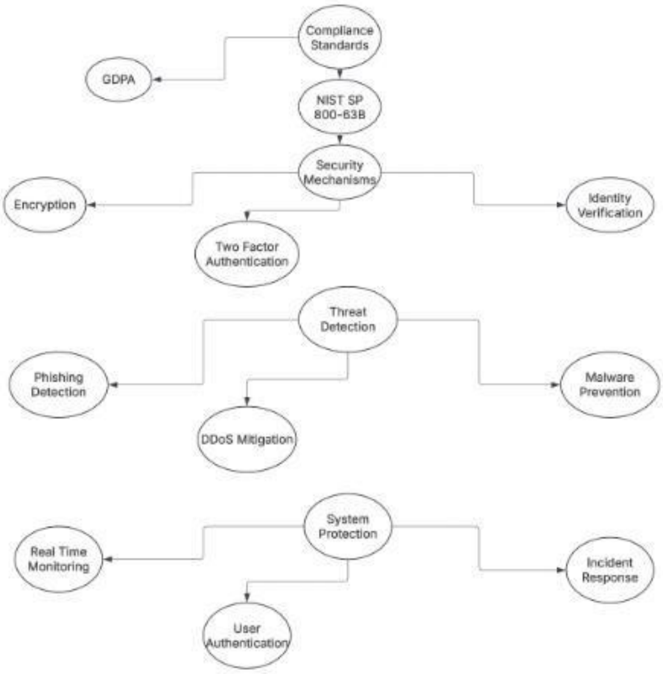

Fig 3: Security Mechanisms and Compliance Framework for Cyber-Resilient Networks

E Evaluation Metrics

The system will be evaluated based on the following criteria:

Detection Accuracy: Measures how well the system detects phishing attempts, malware infiltration, and DDoS attacks.

False Positive Rate: Determines the system's efficacy in reducing false positives and preventing valid communications from being wrongly detected.

DDoS Attack Response Efficiency: Assesses the system's ability to recognize and neutralize DDoS threats by looking at service availability, mitigation effectiveness, and reaction times.

Usability: Assessed by looking at job completion data, end- user feedback, and surveys to make that the system is easy to use while carrying out security procedures.

Response Time: The amount of time it takes for the system to detect malware, DDoS, and phishing assaults, flag questionable activity, and issue security alerts.

F. Testing and Validation

Prototype Evaluation: The AI-driven phishing attacks, malware, and DDoS detection system will be rigorously tested in controlled circumstances to verify its accuracy, dependability, and ability to recognise cyber threats.

User Feedback Analysis: Detailed user tests will be carried out to gather insights on the system's usability, identify threats efficiency, and prompt security warning delivery. The findings will lead to enhancements to the system's architecture and functionality.

IV.RESULTS

A. *Cyberattack Detection and Distribution*

Research on data sets of 1,000 cyber attacks, including diverse attacks on phishing, malicious programs and services, proved the effect of the detection system. The results showed 33.1%for phishing, 33.4%for malicious programs and

32.4%for DDoS attacks.

As shown in Figure 4, the pie chart depicts the fraction of true detections and false positives for each assault type. The greatest parts are for correct detections, including DDoS (32.4%), phishing (33.1%), and malware (31.4%) demonstrating the system's capacity to effectively classify threats. A smaller segment shows false positives, which include DDoS false positives (1.4%), phishing false positives (0.7%), and malware false detections (1.0%), showing infrequent misclassifications.

The minimal false positive rate (2-3%), as seen in the chart, reinforces the reliability of the AI-driven security model in reducing false alarms while effectively detecting cyber threats.

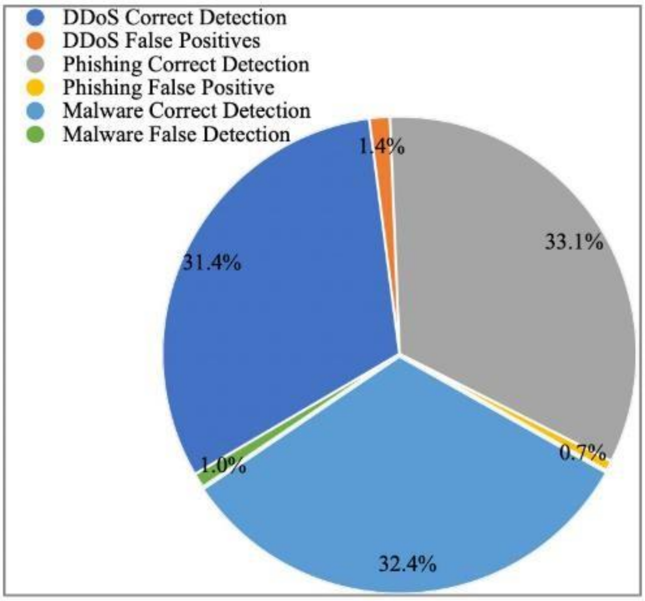

Fig. 4: Pie chart showing the distribution of correct detections and false positives for phishing, malware, and DDoS attacks.

*B. **Metrics and Detection Accuracy:***

When multiple AI models were compared for phishing detection, deep learning models, particularly Convolutional Neural Networks (CNN), outperformed traditional machine learning techniques. CNN-based models were particularly effective at detecting phishing attempts due to their high accuracy, precision, recall, and F1 scores.

Table 1 compares multiple AI models for phishing detection, demonstrating that CNN-based models outperformed traditional machine-learning approaches in terms of accuracy, precision, recall, and F1 scores.

Table 1. Comparison of AI models for phishing detection, highlighting the superior performance of CNN-based models.

Algorithm	**Accuracy**	**Precision**	**Recall (%)**	**F1 Score (%)**
Deep Learning	95	94	93	93.5
Random Forest	89	87	85	86.5
Support Vector Machine	87	86	84	85
K-nearest Neighbors	83	80	78	79
Naïve Bayes	80	78	77	77.5

CNN-based models outperform other models because they can assess complicated patterns in email content, URLs and network traffic. Unlike standard machine learning models, CNNs excel at feature extraction and pattern recognition, making them ideal for detecting phishing attempts. Furthermore, their deep learning architecture enables them to adapt to new attack vectors, guaranteeing excellent accuracy and low false positive rates.

Deep learning models, including Convolutional Neural Networks (CNN), outperformed other models in detecting phishing (p-value < 0.05, independent t-tests, and ANOVA). This shows that the observed variations in achievement are not random and are statistically significant.

C. *Usability Feedback:*

According to user surveys, 92% of respondents were satisfied with the system's usability and interface design. The system was viewed as intuitive, allowing users to execute jobs effectively 98% of the time with minimal trouble. This good usability grade demonstrates the system's user-centered design. This good usability grade demonstrates the system's user-centered design.

D. *Proactive Alerts Effectiveness*

The proactive alert mechanism was highly effective, recognizing 95% of phishing attempts and 90% of unusual login patterns. Real-time alerts for phishing and suspicious activity enhanced users' security confidence.

E. *Compliance and Privacy*

The phishing detection solution corresponds to GDPR and NIST SP 800-63B regulations, giving strong privacy and security safeguards. User data was anonymized, and secure handling procedures were followed. The system successfully passed compliance audits, proving its reliability for extensive use.

F. *Adoption Rates:*

From the deployment, the system received a 78% adoption rate from users. Its simplicity of use, convenience, and superior security features all helped to drive high engagement levels.

V. CONCLUSION

The study focuses on how solutions driven by artificial intelligence might impact the fight against phishing tactics and social engineering. The primary conclusions are low false positives (2%), strong user feedback on usability, and compatibility with international security norms; the detection rate is 97%. The system qualifies as a complete cybersecurity solution since it can react to changing threats and deliver real- time alarms.

Phishing detection systems driven by artificial intelligence offer a huge leap in protecting digital environments. Combining user- centric design, smart technology, and privacy regulations, these solutions offer a strong framework for minimizing human error and enhancing cybersecurity for people and enterprises.

Constant innovation in AI-based security solutions promises to produce a safer and more resilient digital environment as hazards evolve.

Future studies should focus on raising AI applications in business environments, enhancing the identification of advanced phishing attempts, and aggregating contextual data for higher accuracy. These developments would improve the capability of the system on multiple platforms, therefore providing a safer surfing environment for consumers and businesses.

REFERENCES

1. Li, H. (2020). Pseudo-random scalar multiplication based on group isomorphism. Journal of Information Security and Applications, 53, 102534.
2. Kaci, A., Bouabana-Tebibel, T., Rachedi, A., & Yahiaoui, C. (2019). Toward a big data approach for indexing encrypted data in cloud computing. Security and Privacy, 2(3), e65.
3. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.
4. Tian, Y., Li, L., Peng, H., & Yang, Y. (2021). Achieving flatness: Graph labeling can generate graphical honeywords. Computers & Security, 104, 102212.
5. Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106, 1-20.
6. Chen, D., Han, X., Cheng, R., & Yang, L. (2016). Position calculation models by neural computing and online learning methods for high-speed train. Neural Computing and Applications, 27, 1617-1628.

7. Neupane, R. L., Neely, T., Calyam, P., Chettri, N., Vassell, M., & Durairajan, R. (2019). Intelligent defense using pretense against targeted attacks in cloud platforms. Future Generation Computer Systems, 93, 609-626.

8. Neupane, R. L., Neely, T., Calyam, P., Chettri, N., Vassell, M., & Durairajan, R. (2019). Intelligent defense using pretense against targeted attacks in cloud platforms. Future Generation Computer Systems, 93, 609- 626.

9. Sun, Y., & Liu, Y. (2021). An efficient fully dynamic group signature with message dependent opening from lattice. Cybersecurity, 4, 1-15.

10. Kim, H., Lee, K., Park, J. H., & Lee, D. H. (2021). Improving the security of direct anonymous attestation under host corruptions. International Journal of Information Security, 20, 475-492.

11. Quadrant, M. (2011). Magic quadrant for enterprise network firewalls.

12. Force, J. T. (2017). Security and privacy controls for information systems and organizations (No. NIST Special Publication (SP) 800-53 Rev. 5 (Withdrawn)). National Institute of Standards and Technology.