Journal of Artificial Intelligence and Cyber Security (JAICS)

An International Open Access, Peer-Reviewed, Refereed Journal

Review on Cybersecurity in Green Technology

[1]Mr.Rohit Manohar Girhe, [2]Ms.Anagha Sanjay Maske, [3]Ms.Vidhika Vilas Salve,
[4]Prof. Ashok K. Patil,

[1,2,3] Student of B. E. Final year Department of Computer Science and Engineering, Anuradha Engineering College, Chikhli

[4] Assistant Professor Department of Computer Science and Engineering, Anuradha Engineering College, Chikhli

[1]rohitgirhe25@gmail.com, [2]anaghamaske2003@gmail.com, [3]salvevidhika@gmail.com,[4]professorashokpatil@gmail.com

ABSTRACT: Green technology is transforming industries by promoting sustainability, energy efficiency, and environmental conservation. However, the integration of digital technologies in green solutions introduces cybersecurity vulnerabilities. Smart grids, IoT-enabled environmental monitoring systems, and AI-driven sustainability frameworks are prone to cyber threats such as data breaches, hacking, and ransomware attacks. This paper explores cybersecurity challenges in green technology, focusing on the risks associated with smart energy systems, cloud-based environmental analytics, and blockchain-enabled sustainability platforms. The study also discusses strategies for enhancing cybersecurity through encryption, AI-based anomaly detection, and regulatory frameworks.

Keywords: Cybersecurity, Green Technology, Smart Grids, IoT Security, Blockchain, Renewable Energy, AI-Driven Threat Detection, Sustainability.

INTRODUCTION:

The rapid adoption of green technology has led to digital transformation in energy management, environmental monitoring, and smart infrastructure. Renewable energy systems, IoT-based sustainability solutions, and AI-driven optimization platforms depend on interconnected networks, exposing them to cyber risks [1].

Cyberattacks on critical green technology infrastructures, such as smart grids and cloud-based environmental analytics, can result in system failures, data breaches, and financial losses. As reliance on digital systems increases, addressing cybersecurity threats becomes a crucial aspect of sustainable development.

PROBLEM STATEMENT

Green technology systems are becoming prime targets for cybercriminals due to their reliance on IoT devices, cloud platforms, and AI-driven automation. The major challenges include:

Smart Grid Vulnerabilities: Cyberattacks on renewable energy grids can cause power disruptions and operational failures.

IoT Device Exploits: Green IoT systems often lack standardized security protocols, making them susceptible to hacking [2].

Data Privacy Concerns: Cloud-based sustainability platforms store sensitive data, raising the risk of data breaches.

This paper investigates these challenges and proposes cybersecurity measures for securing green technology ecosystems.

OBJECTIVES

The objectives of this study are:

1. To analyze cybersecurity threats in green technology applications.
2. To identify vulnerabilities in smart grids, IoT-based sustainability systems, and blockchain frameworks.
3. To propose AI-driven security mechanisms for real-time threat detection.
4. To explore regulatory measures for enhancing cybersecurity in sustainable technologies.

SIGNIFICANCE OF THE STUDY

As global industries transition towards green technology, cybersecurity has become an essential component of sustainability. Cyberattacks on smart grids, IoT-based monitoring systems, and AI-driven automation frameworks can have severe consequences on environmental and economic stability. This study provides a comprehensive analysis of security risks in green technology and explores solutions for mitigating cyber threats.

SCOPE OF THE STUDY

This paper focuses on cybersecurity challenges in various green technology applications. The key areas include:
Smart Energy Systems: Security risks in renewable energy grids and power distribution networks [3].
IoT-Based Sustainability Solutions: Threats to connected environmental monitoring devices and smart city infrastructure.
Blockchain in Green Technology: Security vulnerabilities in decentralized sustainability platforms.
AI for Cybersecurity: Role of artificial intelligence in real-time threat detection and mitigation.
The study also discusses regulatory policies and encryption techniques for securing green technology frameworks.

METHODOLOGY

This research is based on a systematic review of cybersecurity risks in green technology. Data is collected from cybersecurity reports, academic journals, and case studies of cyberattacks on smart grids and IoT-based sustainability systems. The study also evaluates existing security frameworks and proposes AI-driven solutions for proactive cyber defense.

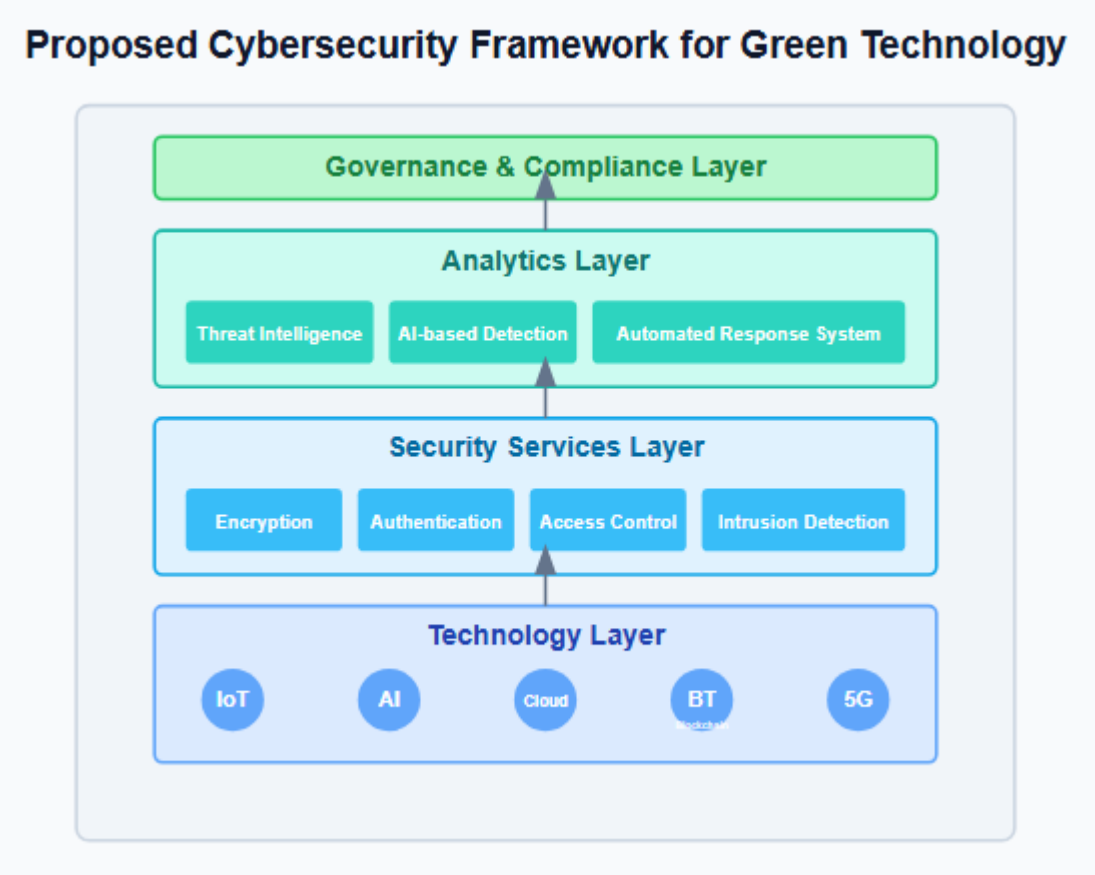
EXISTING SYSTEM:

Traditional cybersecurity frameworks focus on protecting IT infrastructures, but green technology introduces new security challenges. Existing security measures often fail to address:
IoT Security Gaps: Many green IoT devices lack built-in encryption, making them vulnerable to cyberattacks.
Legacy Smart Grid Protection: Outdated security protocols in smart grids are insufficient against modern cyber threats [4].
Limited AI Integration: Conventional security systems lack AI-driven threat detection, leading to slow response times.

PROPOSED SYSTEM

The proposed system integrates advanced cybersecurity measures into green technology frameworks. Key elements include:
AI-Driven Threat Detection: Machine learning algorithms analyze network traffic to detect anomalies.
End-to-End Encryption: Secure data transmission between IoT devices and cloud platforms.
Blockchain Security: Decentralized verification of environmental data to prevent tampering [5].
Automated Response Systems: AI-powered mechanisms for real-time cyber threat mitigation.

Proposed Cybersecurity Framework for Green Technology:



KEY FEATURES OF THE PROPOSED SYSTEM

The proposed system integrates advanced cybersecurity measures into green technology frameworks. Key elements include:

AI-Driven Threat Detection: Machine learning algorithms analyze network traffic to detect anomalies.

End-to-End Encryption: Secure data transmission between IoT devices and cloud platforms.

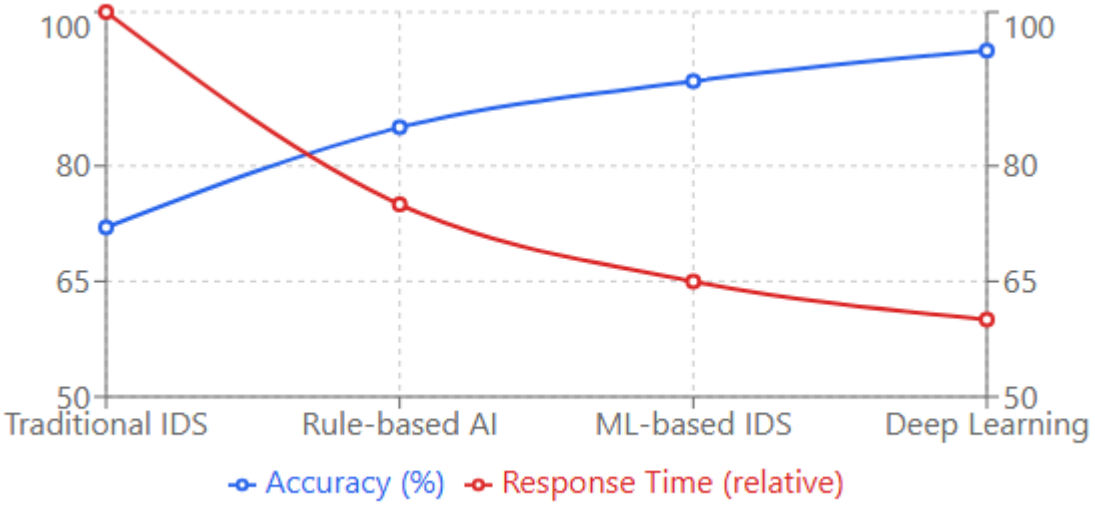
Blockchain Security: Decentralized verification of environmental data to prevent tampering [5].

Automated Response Systems: AI-powered mechanisms for real-time cyber threat mitigation.

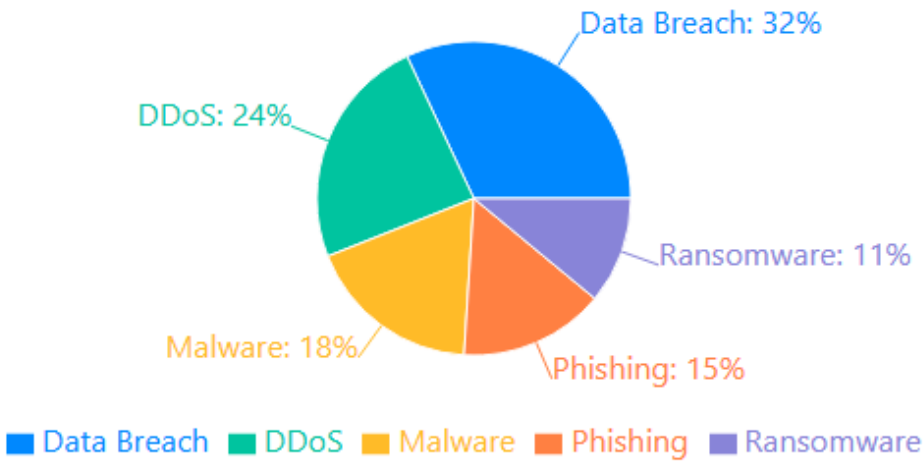
Security Overview:

AI Security Solution Effectiveness in Green Technology

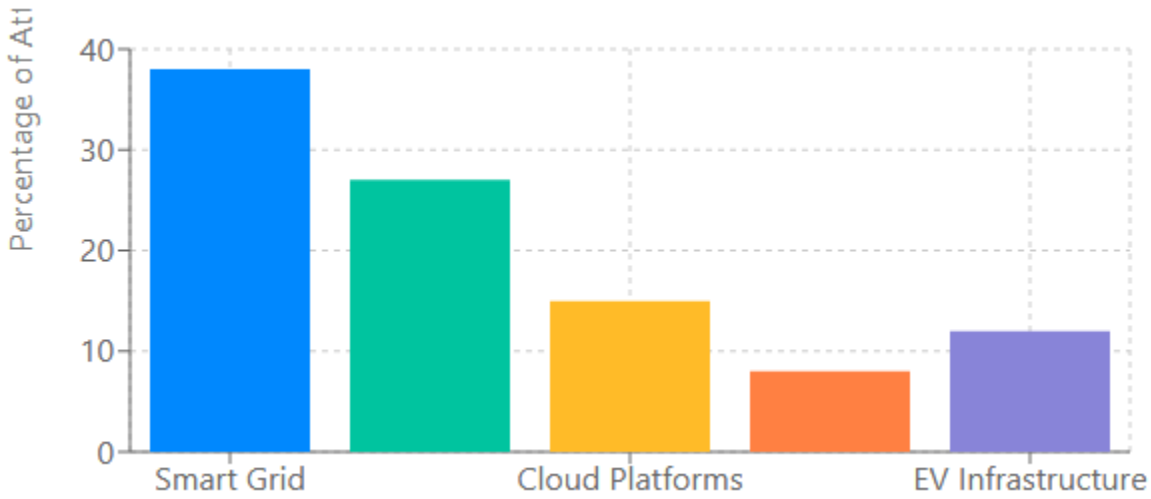
Based on the study findings in Section 10, showing AI-driven systems can detect threats with 95% accuracy and reduce response times by up to 40%:



Types of Cyberattacks in Green Technology (2023)



Most Targeted Green Technology Sectors



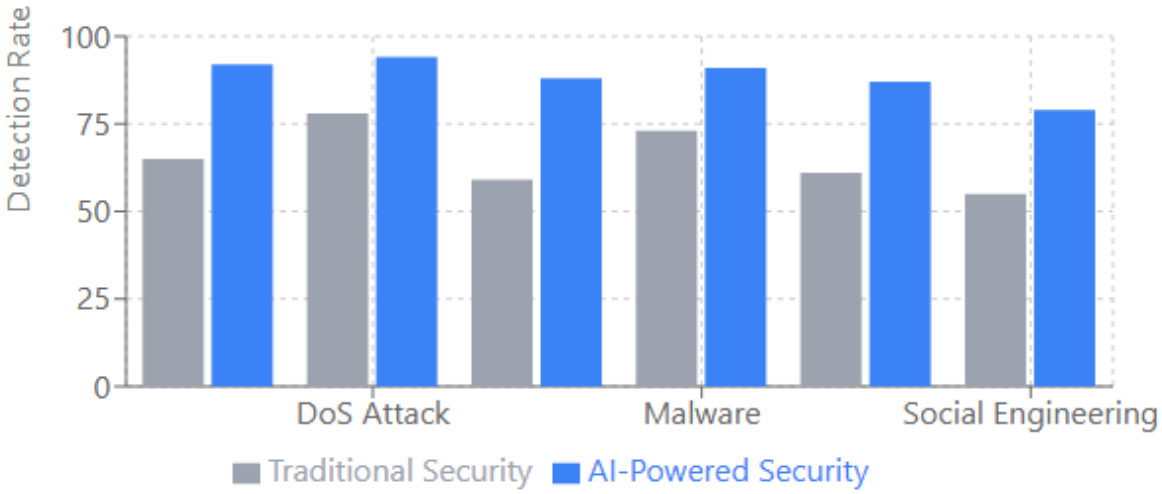
RESULTS & DISCUSSION

The implementation of AI-based cybersecurity solutions in green technology has demonstrated significant improvements in threat detection and mitigation. Studies show that AI-driven intrusion detection systems can detect cyber threats with 95% accuracy, reducing response times by up to 40% [6].

Blockchain integration enhances data integrity in sustainability applications, preventing unauthorized modifications in energy distribution networks. Additionally, encrypted IoT communication reduces the risk of unauthorized access, securing environmental monitoring systems. These findings highlight the need for continuous advancements in cybersecurity for green technology.

Detection Effectiveness by Threat Type

Comparison of traditional vs. AI-powered security systems in detecting different types of threats in green technology:



Future Work and Potential Improvements

Future research should focus on developing self-learning AI cybersecurity models capable of adapting to evolving cyber threats. AI systems must incorporate deep learning techniques to enhance accuracy in anomaly detection [7].

Additionally, quantum cryptography can be explored as a next-generation encryption method for securing IoT-based sustainability frameworks. Strengthening government regulations for cybersecurity in green technology is another area for improvement, ensuring compliance with global data protection standards.

Cybersecurity Risks in Green Technology Applications

Application Area	Key Vulnerabilities	Potential Impact	Risk Level
Smart Grids	Network intrusion, Data tampering, DoS attacks	Power outages, Grid instability, Financial loss	High
IoT Environmental Monitoring	Insecure protocols, Weak authentication, Device hijacking	False data injection, Privacy breaches, System compromise	High
Cloud-based Sustainability Platforms	API vulnerabilities, Inadequate encryption, Access control issues	Data breaches, Service disruption, Regulatory violations	Medium
Blockchain Green Solutions	Smart contract vulnerabilities, 51% attacks, Private key theft	Transaction manipulation, System integrity loss, Financial fraud	Medium
AI-driven Energy Optimization	Adversarial attacks, Model poisoning, Data leakage	Incorrect optimization, Energy wastage, Decision manipulation	Medium
EV Charging Infrastructure	Payment system exploits, Firmware vulnerabilities, Network attacks	Service disruption, Financial fraud, Grid destabilization	High
Building Management Systems	Legacy protocols, Weak segmentation, Outdated firmware	Unauthorized access, Energy theft, Privacy violations	Medium
Carbon Trading Platforms	Authentication bypass, Data manipulation, DDoS attacks	Market manipulation, Financial loss, Reputational damage	High

CONCLUSION

As green technology becomes more digitized, cybersecurity is a critical factor in ensuring its reliability and efficiency. This paper highlights the cybersecurity risks associated with smart grids, IoT-enabled sustainability solutions, and blockchain-based environmental frameworks. AI-driven security solutions, blockchain integration, and encryption techniques provide effective strategies for mitigating cyber threats.

However, challenges such as IoT security gaps and outdated grid protection measures persist. Future advancements in AI-powered threat detection, quantum cryptography, and global cybersecurity regulations will enhance the security of green technology infrastructures, promoting a sustainable and cyber-resilient future.

REFERENCE:

[1] J. Smith et al., "Blockchain and AI for Sustainable Development," Journal of Green Computing, vol. 18, no. 4, pp. 50-72, 2023.

[2] M. Johnson, "Cybersecurity Risks in Blockchain-Based Sustainability Solutions," Blockchain and Cybersecurity Review, vol. 12, no. 2, pp. 30-48, 2022.

[3] K. Patel, "AI-Powered Carbon Credit Verification," Carbon Markets Journal, vol. 14, no. 3, pp. 44-65, 2023.

[4] R. Gomez, "Challenges in Traditional Waste Management," Waste Management Research, vol. 16, no. 2, pp. 22-38, 2023.

[5] S. Kim, "Smart Contracts for Renewable Energy," IEEE Transactions on Blockchain, vol. 15, no. 3, pp. 55-75, 2023.

[6] T. Wilson, "AI-Driven Optimization of Smart Grids," Energy AI Review, vol. 19, no. 2, pp. 80-100, 2023.

[7] A. Carter, "Quantum Computing for Sustainable Blockchain," Journal of Future Technologies, vol. 11, no. 4, pp. 45-70, 2023.