Journal of Posthumanism
2023
Volume: 3, No: 3, pp. 333–350
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v3i3.2585
Submission Date: November 15, 2023
Publication Date: December 04, 2023

Developing Predictive AI Models for Securing U.S. Critical Infrastructure Against Emerging Cyber Threats

Anupom Debnath[1], Sadia Sharmin[2], Nur Vanu[3], Adib Hossain[4], Muslima Begom Riipa[5], Anseena Anees Sabeena[6], Md Azharul Islam[7], Arafat Islam[8], Sanchita Saha[9]

Abstract

Smart grids (SGs) have emerged in the United States as part of the effort to modernize the nation's aging electricity infrastructure. While existing cybersecurity tools are generally effective at detecting and preventing known threats, they fall short in addressing the growing complexity of advanced cyberattacks. Ensuring robust protection for the U.S. smart grid requires a comprehensive approach that integrates advanced technologies and proactive processes. Leveraging big data analytics, artificial intelligence (AI), and machine learning (ML) enables a more adaptive and holistic security framework. These technologies allow for the identification of new, previously undetected threats by analyzing behavioral patterns and predicting anomalies through intelligent systems. By combining known and unknown threat data, predictive analytics can significantly enhance the cybersecurity posture of critical energy infrastructure. This paper explores current trends and key challenges in safeguarding U.S. smart grids using big data and AI-driven approaches. It includes an overview of smart grid architecture and functionality, highlights technological advancements, and outlines a qualitative risk assessment method. Additionally, it discusses major contributions to improving the reliability, safety, and efficiency of the electric grid, proposes layered security measures, and evaluates cybersecurity risk management strategies for supervisory control and data acquisition (SCADA) systems.

Keywords: *Smart Grid, Cybersecurity, Artificial Intelligence, Machine Learning, Big Data Risk Assessment*

Introduction

The concept of a "smart and sustainable city" is gaining momentum across the United States, driven by two primary goals: improving energy management through smart electricity grids that support renewable energy, and promoting efficient mobility solutions to reduce reliance on personal vehicles and curb greenhouse gas emissions. While information and communication

[1] Department of Business Administration, International American University, Los Angeles, CA 90010, USA; Email: debnathanupom05@gmail.com
[2] Department of Business Administration, International American University, Los Angeles, CA 90010, USA; Email: sadiasharminlglg@gmail.com
[3] Department of Science in Business Analytics, Trine University, Angola, IN 46703, USA; Email: nurvanu94@gmail.com
[4] Department of Business Analytics, Trine University, Angola, IN 46703, USA; Email: adibhossain998@gmail.com
[5] Department of Business Administration, International American University, Los Angeles, CA 90010, USA; Email: mbriipa@gmail.com
[6] Department of Business Administration, Westcliff University, Irvine, CA 92614, USA; Email: anseenaaneessabeena@gmail.com
[7] Department of Business Administration, Westcliff University, Irvine, CA 92614, USA; Email: m.islam.552@westcliff.edu
[8] Department of Business Analytics, Trine University, Indiana, USA; Email: arafatislamdha@gmail.com
[9] Department of Business Administration, Westcliff University, Irvine, CA 92614, USA; Email: s.saha.552@westcliff.edu

technologies (ICT) play a central role in this transformation, they are tools—not ends in themselves. The real objective is to use ICT to reduce the environmental impact of urban living while enhancing the quality of life for American citizens. As U.S. cities continue to grow in size and density, addressing the associated environmental and infrastructural challenges becomes increasingly urgent [1].

In the U.S., the electricity sector is transitioning toward a modern, automated, and sustainable distribution system. With rising expectations for more connected and integrated operations, utility providers are under pressure to ensure a consistent and efficient power supply. SG technology is critical to this evolution, allowing for better integration of renewable energy sources and enabling bidirectional energy flow [2]. These systems also improve real-time monitoring and management at the distribution level, helping utilities optimize current infrastructure rather than building new power plants [3].

Smart grids in the U.S. are designed to support both centralized and distributed energy generation, enhancing the grid's flexibility and resilience. This decentralization reduces vulnerability during emergencies or disasters by limiting the number of high-value targets such as large fossil-fuel-based power plants [4]. Environmentally, the adoption of smart grid technologies plays a key role in lowering carbon emissions by promoting clean, distributed generation—especially through solar and hydroelectric systems—and reducing dependence on centralized fossil-fuel sources [5].

Cybersecurity remains a significant concern as the American grid becomes more digitized and interconnected. A thorough analysis of cybersecurity threats in smart grid systems—particularly embedded systems—is essential to understanding potential attack vectors [6]. Techniques such as game theory and coordinated threat modeling offer frameworks to predict and counteract cyber threats. U.S. energy sector associations are actively engaged in managing these risks while ensuring that core power supply functions remain uninterrupted [7].

A major contributor to the enhanced reliability, safety, and efficiency of U.S. electrical infrastructure is the application of intelligent optimization algorithms. Tools like neural networks, genetic algorithms, reinforcement learning, and support vector machines are increasingly being used to improve system performance and analyze demand in energy markets [8]. These AI-driven approaches help quickly identify critical infrastructure components and strengthen grid security.

In the cybersecurity context, the International Organization for Standardization defines it as preserving the confidentiality, integrity, and availability of data within cyberspace. Cyberspace itself is characterized as a complex, non-physical network formed by the interaction of people, software, and services through connected devices [9]. This paper presents a detailed analysis of smart grid architecture and cybersecurity concerns in the U.S., emphasizing the importance of AI and big data. It also introduces a risk-based cybersecurity framework grounded in industry standards and best practices, providing guidance for American SG operators in managing cyber risks effectively.

The paper is organized as follows: Section 2 explores the role of energy management in building smart, sustainable U.S. cities. Section 3 identifies key cybersecurity threats facing smart grids. Section 4 delves into securing smart grid infrastructures using big data and AI. Section 5 reviews current risk modeling techniques, while Section 6 highlights the most effective strategies for mitigating cyber-attack risks in smart grid systems. Section 7 offers concluding remarks on the future of smart grid cybersecurity in the United States.

Energy Management in Smart Sustainable Cities

Building a smart and sustainable city in the United States is a complex and evolving process that demands collaborative governance involving local governments, private companies, researchers, and engaged citizens. As urban areas become more connected and data-driven, significant research and planning are needed to define how these systems can best function [10, 11]. The concept is appealing, especially as it aligns with the goals of improving quality of life, addressing environmental challenges, and enhancing operational efficiency in American cities. While digital technologies and information systems are central to this transformation, they are tools—not the ultimate goal. The real purpose is to make U.S. cities more livable, efficient, environmentally responsible, and inclusive for all residents.

As urbanization accelerates, the stakes are growing. By 2025, an estimated 58% of the global population will live in cities, with the rate reaching nearly 80% in developed countries like the U.S. By 2050, urban dwellers will comprise around 75% of the world's population [12]. American cities, already facing challenges like congestion, rising energy demands, climate change, and environmental degradation, must take proactive steps to remain sustainable and resilient. Urban centers consume approximately 65% of all primary energy and contribute about 70% of global greenhouse gas emissions—primarily due to the energy needs of buildings and transportation systems [13]. These realities make strategic urban planning and energy management critical to a more sustainable future.

Among various smart city initiatives, energy management stands out as a top priority for many U.S. municipalities. Addressing both environmental and economic concerns, smart energy solutions can reduce carbon emissions while helping residents and businesses cut utility costs. One of the most promising advancements in this area is the implementation of smart grids. Using smart meters and embedded sensors, cities can monitor real-time energy consumption across residential and commercial buildings [14]. This detailed data enables utility providers and city planners to identify peak usage periods and take steps to balance loads—such as temporarily disconnecting non-essential devices during high-demand hours.

In addition to improving energy efficiency, smart grids support the integration of renewable energy sources like wind, solar, cogeneration, and geothermal power. Through decentralized energy production and the use of modern storage solutions—such as batteries—cities can store excess power generated during the day and redistribute it during high-demand periods [15]. For example, solar panels on office buildings can charge storage systems during daylight hours, with the stored energy later used in nearby homes after business hours. Furthermore, electric vehicles can play a dual role, serving as mobile storage units that feed electricity back into the grid when needed or recharge during off-peak hours.

In the U.S., these technologies not only advance environmental goals but also empower consumers by giving them access to real-time consumption data. This transparency encourages energy-saving behavior and supports broader sustainability efforts. As more American cities embrace smart energy infrastructure, they move closer to achieving a future that is cleaner, more efficient, and better equipped to meet the challenges of rapid urbanization and climate change.

Security Threats in Smart Grids

The reliability of smart grids in the United States hinges on maintaining trust, secure communication, and constant availability of control systems that manage the grid's operations [16]. As part of the smart grid ecosystem, big data plays a pivotal role by processing vast datasets across devices and networks to generate actionable insights that inform real-time decision-making and long-term planning. The architecture of big data systems—comprising hardware, software, networking, and data-handling technologies—demonstrates how these components integrate to support the operational goals of intelligent power systems.

However, integrating ICTs into the smart grid introduces new vulnerabilities [17]. Data transmitted between devices often travels through the public internet using standard Internet Protocol (IP), which carries known security flaws that can open the door to cyber intrusions or data interceptions [18]. These vulnerabilities highlight the critical need to protect and secure information within the grid. At the heart of smart grid cybersecurity is the CIA triad—confidentiality, integrity, and availability—which defines the core security requirements necessary for maintaining safe and reliable operations.

Understanding these requirements is essential before implementing cybersecurity frameworks. First, availability ensures timely and reliable access to data. Any interruption in availability can disrupt energy distribution and management, weakening the grid's operational capacity. Second, integrity refers to protecting data from unauthorized alterations or destruction, ensuring authenticity and non-repudiation. Finally, confidentiality involves restricting access to sensitive data, preventing unauthorized disclosure that could compromise consumers or system operations. Table 1 further elaborates on the cybersecurity threats associated with each of these core principles.

To address these threats in the context of the U.S. smart grid, the National Institute of Standards and Technology (NIST) has issued detailed recommendations covering both cybersecurity and physical infrastructure protections [19]. Several key requirements emerge for communication networks within intelligent power systems. Privacy protection is especially critical, as smart meters and load monitoring tools can inadvertently reveal detailed usage patterns. These patterns may be exploited by malicious actors to infer occupancy in homes or identify high-usage sites, making consumers vulnerable to targeted attacks. While privacy technologies have matured, the appropriate solution depends on the communication system in use.

Another vital security feature is the ability to detect attacks and respond swiftly. Given the extensive reach of smart grid networks, it is nearly impossible to secure every node [20]. Therefore, continuous profiling, traffic monitoring, and anomaly detection are necessary to quickly identify and respond to suspicious activity. Additionally, the continuity of operations must be prioritized. Smart grid systems should be able to maintain or resume functionality even in the face of cyber disruptions. This includes developing comprehensive contingency plans, alternative control strategies, data recovery protocols, and regular failure response testing.

Identification, authentication, and access control mechanisms are equally essential. With millions of smart devices connected across the grid, verifying the identity of users and devices is critical for controlling access to sensitive resources. Each network node must be equipped with cryptographic capabilities to manage authentication and encrypt data effectively [21]. Furthermore, audit and accountability systems must be in place. Regular audits are needed to uncover weaknesses, monitor data logs, and analyze system events—such as unexpected outages—to understand the root causes and improve future resilience.

In summary, securing the smart grid in the U.S. requires a layered approach informed by rigorous standards, such as those outlined by NIST, and supported by advanced technologies in data analytics, encryption, and intrusion detection. Table 1 in the article outlines how each component of the CIA triad aligns with specific threat types, providing a framework for developing comprehensive, risk-based cybersecurity solutions for the nation's evolving electrical infrastructure.

According to Threat	Security Objective	Affected	Active or Passive	Examples
Interception	Confidentiality	Passive	Usually, cannot be detected but can be prevented with cryptography	Denial of services (DoS), data traffic monitoring
Modification	Integrity	Active	Can be detected with cryptography	Modification of control signals, sensor data, energy use information
Interrupt	Availability	Active	Can be detected but usually not prevented	Elimination of routing, deleting data, software modification
Manufacturing	Authenticity	Active	Can be detected with cryptography	Saturation attacks, false control signals, bogus financial transactions

Table 1: Malicious attack on the smart grid [22]

Security-Aware of SG Infrastructures in Era of Big Data and Artificial Intelligence

In the United States, one of the most common points of vulnerability within smart grids lies in smart meters—devices that directly interface with electricity supply and demand. These vulnerabilities often depend on the geographic location of meter installations and the strength of the encryption algorithms used to analyze energy consumption data [23, 24]. As the U.S. electrical infrastructure continues to evolve, smart grids represent the integration of advanced information technologies into power systems. This digital transformation allows for more efficient, automated operations that benefit both utility providers and consumers, all while aiming to ensure a stable and continuous energy supply.

However, many Supervisory Control and Data Acquisition (SCADA) systems currently in use were implemented decades ago, prior to the establishment of modern cybersecurity standards [25]. Originally, SCADA designers did not view cybersecurity as a critical issue, given that these systems were not connected to the internet. Over time, however, SCADA systems have become internet-accessible—often without proper security protections—making them susceptible to cyber threats. Replacing outdated SCADA systems with more secure alternatives is urgently needed, but such upgrades involve significant financial investment, which often leads to delays in implementation.

To enhance protection at larger facilities, it's essential to secure the SCADA network from internal threats. One effective measure is installing an additional firewall between the corporate network and the SCADA environment. This barrier enforces stricter security protocols, allowing authorized engineers to perform maintenance tasks such as applying security patches, reviewing system logs, and deploying updates without compromising system integrity.

Communication technologies used in smart grid applications—particularly within domestic area networks, neighborhood area networks (NANs), and wide-area networks—have also received attention in cybersecurity research. For example, Bekara examined the security issues in smart grids built on Internet of Things (IoT) frameworks and outlined critical security services necessary for protection [26]. Over time, the scope of IoT has expanded to include a variety of technologies such as wireless sensor networks, machine-to-machine (M2M) communications, ZigBee, WiFi, Narrowband IoT (NB-IoT), LTE, and Bluetooth. These technologies collectively support the digital backbone of the modern U.S. electrical distribution system. As shown in **Figure 1**, this diverse ecosystem of communication and information technologies plays a crucial role in the functioning and security of smart grids.

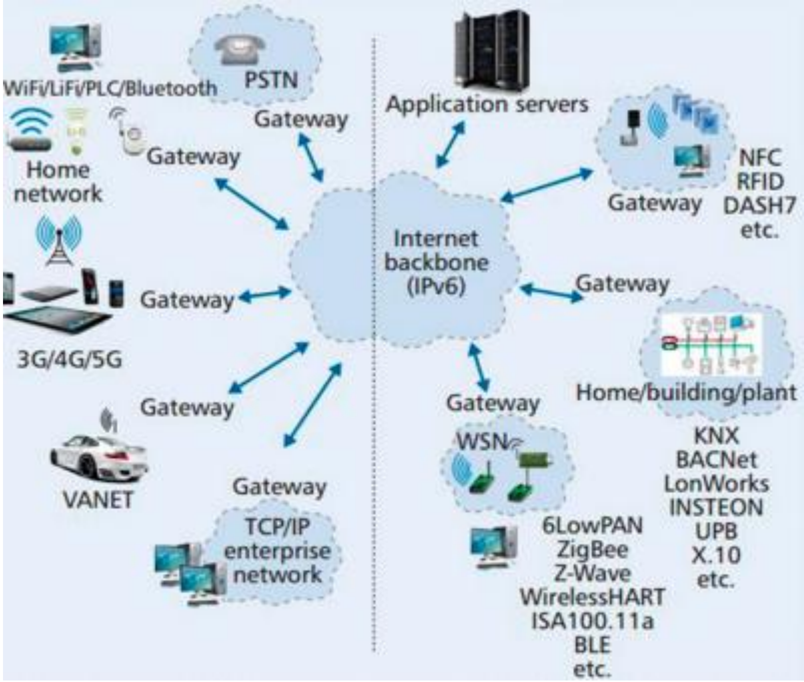

Figure 1: A wide range of information and communication technologies [22]

The Enormous Potential of Big Data

In today's digital era, data has overtaken crude oil as the world's most valuable resource, a sentiment famously captured by *The Economist* in its May 6, 2017 cover story. Within the U.S. smart grid ecosystem, big data plays a transformative role by enabling real-time and predictive insights that drive smarter energy management. Although there's no universally accepted definition of "big data," the term generally refers to massive datasets that exceed the capabilities of traditional software tools and require advanced methods for storage, analysis, and visualization. As illustrated in **Figure 2**, challenges include not only managing the size and complexity of these datasets but also ensuring their secure acquisition, transmission, and maintenance.

Smart grids in the United States are increasingly leveraging advanced algorithms capable of forecasting electricity consumption based on weather patterns and production trends. This forward-looking capability allows utilities to maintain a comprehensive, real-time view of the energy supply and demand landscape. The true strength of smart grid systems lies in their ability to automatically balance energy flows, prioritizing the delivery of power from renewable sources to areas of high demand.

U.S. electricity providers are actively advancing two major data initiatives: first, the expansion of big data infrastructure to handle the growing volume of digital information, and second, the promotion of open data policies that allow this information to be shared and reused without technical restrictions. These strategies support greater transparency, innovation, and efficiency in energy distribution and grid operations [27].

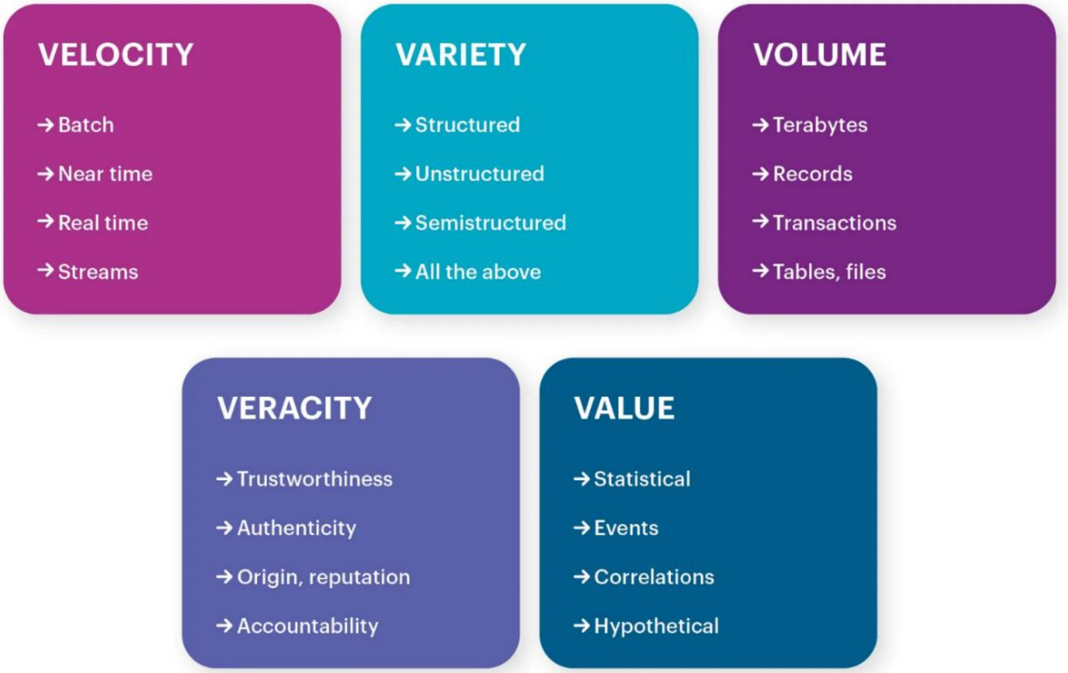

Figure 2: The properties of big data

Cybersecurity and Artificial Intelligence

AI has become an essential component of cybersecurity in the United States' smart grid infrastructure. While technologies like ML, natural language processing (NLP), and robotic process automation (RPA) are often associated with digital manufacturing, they have long been embedded in cybersecurity practices. A classic example is the spam filter, which has utilized machine learning techniques since the early 2000s to adapt to evolving threats [28]. Today, these technologies are far more sophisticated and play a critical role in protecting critical infrastructure.

In modern smart grid systems, AI is being applied to a range of security challenges including fraud detection, malware identification, intrusion detection, risk analysis, and user behavior monitoring. These AI applications help utilities quickly interpret potential threats and reduce response times, thereby maintaining compliance with national cybersecurity standards. Alongside AI, technologies like 5G are further strengthening digital defense capabilities, although continued investment is necessary to stay ahead of emerging cyber threats [29].

AI is also instrumental in intrusion prevention—guarding against both external and internal breaches. Deep learning (DL) models are increasingly used to monitor user accounts, flagging unusual activity such as access from multiple geographic locations in a short period, odd working hours, or unexpected database usage [30, 31]. Meanwhile, machine learning enhances grid resilience by identifying patterns in large datasets, enabling systems to learn from past incidents and improve over time.

By harnessing cyber threat intelligence, smart grid operators in the U.S. can respond more quickly and confidently to incidents [32]. However, current cybersecurity tools are largely designed to identify known threats and often fall short when faced with advanced, stealthy, or zero-day attacks. To combat these evolving threats, there is a growing need for more flexible, data-driven defense mechanisms. Predictive analytics and AI-based behavioral models offer the ability to analyze datasets holistically and detect previously unknown threats. This integrated approach—combining known and emerging threat data—has the potential to revolutionize cybersecurity across America’s smart grid landscape. The specific ways AI enhances cybersecurity in smart grids are outlined in **Table 2**.

How AI Can Help in Cybersecurity	References
Automated Detection	[33, 34]
Quick Identification Errors	[35]
Secure Authentication	[36, 37]
Faster Response Times	[38]
Cybersecurity without Errors	[39]

Table 2: AI and cybersecurity [22]

Survey on Risk Modeling Techniques

To keep up with the increasing sophistication of AI-driven cyberattacks, electric utility companies in the United States are increasingly compelled to adopt similarly advanced technologies in their cybersecurity strategies [40]. Many AI-based security solutions are now widely available, especially in the area of endpoint protection. Unlike traditional signature-based security systems, which rely on known threat profiles, modern solutions use dynamic behavior analysis, enhanced with machine learning and intelligent automation, to identify threats in real-time [41]. These advanced systems can detect malicious code within seconds of execution and automatically block it before any harm occurs. Machine learning ensures these platforms are constantly evolving, as they continuously learn from newly identified threats and update their detection capabilities accordingly [42].

Despite these advancements, cybercriminals continue to inflict significant financial losses using conventional attack methods. This underscores the urgency for adopting AI technologies within U.S. smart grid systems. The most progressive research in this field combines electrical engineering advancements, energy storage innovations, big data analytics, cutting-edge ICT, wireless communication systems, and machine learning models [22]. These integrations have also enabled advanced fault management systems, allowing for seamless coordination through local automation. As a result, these sophisticated systems are increasingly relied upon to safeguard critical infrastructure and ensure service continuity, especially for priority users. Given the mission-critical nature of grid operations, diagnostic systems within smart grids must be highly fault-tolerant to quickly detect and resolve anomalies.

CORAS Method for Security Risk Analysis

This study employs a literature review to explore a range of security modeling techniques applicable to smart grid protection in the U.S., with a particular focus on the CORAS method for conducting structured security risk analysis. The application of this method is illustrated in **Figure 3**.

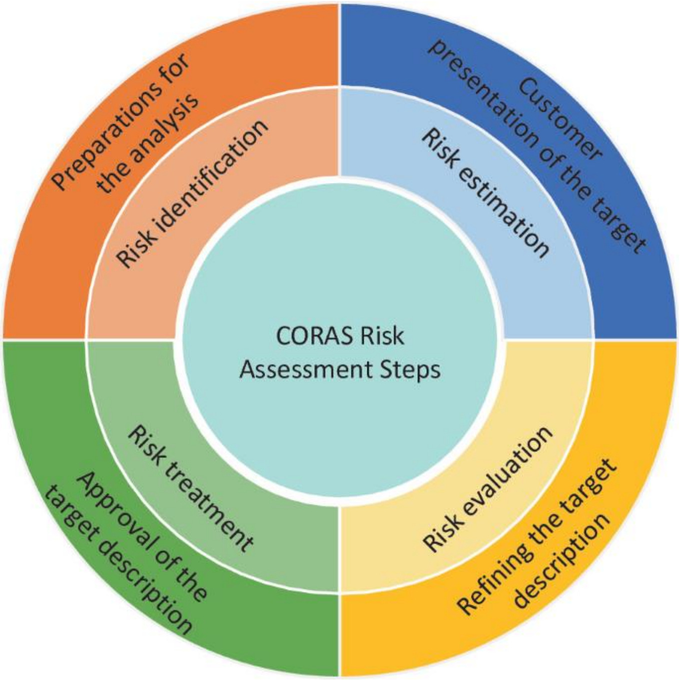
Preparations for the analysis
Customer presentation of the target
Risk identification
Risk estimation
CORAS Risk Assessment Steps
Risk treatment
Risk evaluation
Approval of the target description
Refining the target description

Figure 3: CORAS method for security risk analysis

The review process involved searching electronic databases such as IEEE Xplore and SpringerLink using a combination of qualitative and quantitative approaches. Constructing comparative datasets required meticulous keyword selection and filtering. Among the keywords used were “attack tree security,” “vulnerability analysis,” “false data injection attack detection,” “malicious behavior detection,” “deep learning detection of electricity theft cyber-attacks,” “fraud detection,” “bow tie security,” “anomaly detection method,” “smart grids cyber-attack defense,” and “CORAS security.” These search results formed the basis for a comparative database used to assess high-level quality indicators. The number of relevant publications associated with each keyword is summarized in **Table 3**.

Attacks	References
Switching Attacks	[39]
DoS (Denial of Service)	[43]
Fraud Detection	[44]
Cyber Threat Detection	[45]
Data Integrity	[46]
Replay	[47]
Packet Dropping	[48]
Dynamic Load Altering Attack	[49]
Data Injection Attacks	[50]
Malicious Software (Malware)	[51]
Vulnerability Analysis	[52]
Anomaly Detection	[53]

Table 3: Classification based on security requirements [22]

Cyber Security Risk Assessment Methods for SCADA Systems

This section adopts a qualitative approach to examine a variety of cybersecurity risk assessment methodologies applied to Supervisory Control and Data Acquisition (SCADA) systems in U.S. electric utilities. The goal is to evaluate which methods are most suitable for addressing existing vulnerabilities, while also identifying current shortcomings and areas for improvement. The analysis covers a wide spectrum of techniques, including those focused on wireless sensor network-based threat detection, temporal pattern recognition, CPI-enabled firewall designs, and intrusion detection methods enhanced by machine learning and social media analytics. Other approaches address secure implementations of SCADA communication protocols, hybrid cloud-based SCADA architectures to support microgrid interoperability, and simulations for critical infrastructure vulnerability analysis. Additionally, techniques like pre-distribution key schemes, mobile ad hoc network integrations, and optimization-based intrusion detection algorithms are examined. These methods collectively offer insight into maintaining secure and resilient SCADA operations across interconnected smart grid platforms in the U.S. A comprehensive summary of all twelve methods discussed in this section is provided in **Table 4**.

Method	References
Analysis, classification, and detection methods of attacks through wireless sensor networks	[54]
Detection of cyberattacks using temporal pattern recognition techniques	[53]
CPI-enabled firewall model for SCADA security in smart grid networks	[55]
Combining ensemble methods and social media metrics to improve the accuracy of OCSVM in intrusion detection in SCADA systems	[56]
Vulnerability Analysis	[57]
Data Integrity for cloud-based private SCADA architecture	[58]

Simulation and Malicious Software (Malware)	[59]
Replay and pre-distribution key scheme	[60]
Packet Dropping and attack-resistant SCADA system	[61]
Dynamic Load Altering Attack	[62]
Data Injection Attacks using deep belief	[63]
Anomaly Detection and optimization for intrusion detection	[64]

Table 4: Cyber security risk assessment methods for SCADA systems

Mitigating the Risk of Cyber Attack on Smart Grid Systems

In the United States, defending smart grid systems against modern cyber threats requires close collaboration among engineers, IT professionals, consumers, and security managers. Only by sharing knowledge and insights can these stakeholders effectively identify potential vulnerabilities and emerging threats. Cybersecurity strategies must continuously evolve to address not only current attack vectors but also anticipate future challenges. This means utilities must treat cybersecurity as an ongoing, dynamic process—one that integrates organizational structure with well-defined processes and policies.

Traditional multi-layered security approaches are no longer sufficient to address the sophistication of modern cyberattacks. Today's adversaries design their attacks to bypass standard defenses by learning from existing detection rules. Furthermore, insider threats—attacks initiated by individuals with legitimate access—remain difficult to detect using conventional tools. As a result, U.S. utilities must turn to AI and advanced big data analytics to improve their cybersecurity posture. These technologies provide predictive insights and real-time threat detection capabilities that exceed human capacity, allowing for quicker and more precise responses to cyber incidents.

AI is already embedded in many cybersecurity solutions used in the U.S. energy sector, including antivirus software, endpoint detection and response (EDR) systems, firewalls, and data loss prevention tools. These tools can automatically detect and block malicious activity, significantly reducing the risk of system compromise. However, managing vulnerabilities remains a significant challenge. As the number of published vulnerabilities grows each year, utility companies face increasing pressure to assess real risks, prioritize threats, and automate patch deployments. Not all vulnerabilities are actively exploited, and many systems are safeguarded behind perimeter defenses. Still, the sheer scale and complexity of modern infrastructures demand smarter, AI-integrated solutions.

To address this, many vendors now incorporate AI into their vulnerability management platforms. These systems enhance the discovery of active devices, perform thorough vulnerability scans, evaluate associated risks based on threat intelligence, and assist in prioritizing and automating patch deployment. The goal is to reduce manual workload while increasing the accuracy and efficiency of risk mitigation.

Establishing a strong cybersecurity culture also requires a robust awareness and response program tailored to the smart grid environment. As illustrated in **Figure 4**, this involves several interlinked strategies. One essential component is secured remote access. Simply using usernames and passwords is inadequate; instead, encrypted virtual private networks (VPNs) should be implemented to safeguard remote connections. Given the diversity of operations across electric utilities, there is no universal solution—each security program must be tailored to specific organizational needs and technical contexts.

Another critical element is traffic control. Implementing strict firewall rules can segment internal IT systems from operational technology (OT) environments and specify which systems can communicate and through which protocols. For example, limiting communication between IT and OT systems strictly to HTTPS can block threats that rely on alternative protocols, such as server message block (SMB) attacks.

Risk assessment forms the foundation of any effective cybersecurity program. By evaluating internal and external threats, utility companies can better understand where they are most vulnerable and develop policies to address these risks. These policies should inform all stakeholders—including employees and third-party vendors—of their roles in protecting digital assets and define clear consequences for violations. Maintaining an effective policy also involves regularly scheduled reviews to adapt to evolving threats.

Once policies are in place, utilities must implement projects aligned with internationally recognized cybersecurity standards. Deep packet inspection (DPI) is another critical tool, allowing utilities to analyze data transmissions in real time. DPI helps identify abnormal values or communications that deviate from expected behavior. After a learning phase, systems establish a baseline of normal operation. Any deviation—whether caused by a failing sensor, an unauthorized device, or malware—triggers an alert, enabling rapid response before significant damage occurs.

Altogether, these measures illustrate a comprehensive, AI-driven approach to reducing cyber risks in the U.S. smart grid sector. As utility systems become more interconnected and reliant on data, deploying flexible, intelligent cybersecurity solutions is essential to ensuring long-term resilience and operational continuity.

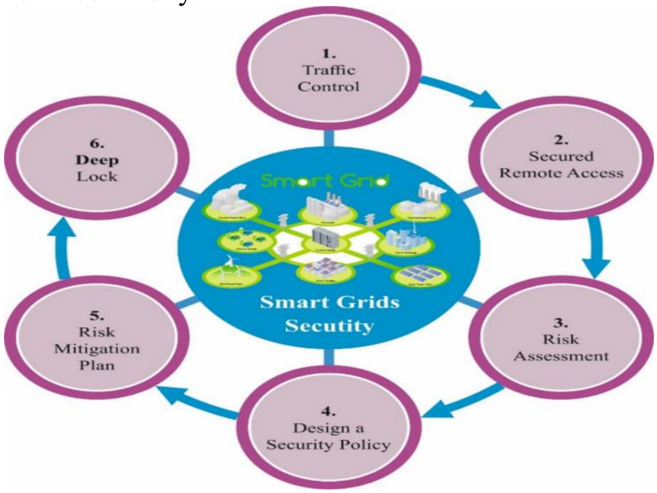

Figure 4: Mitigating the risk of cyber-attack on smart grid systems

Conclusion

The foundational concept of the smart grid alone is not sufficient when implementing such a complex and evolving system, particularly in the United States. Despite advancements in technology and prior experience, building an ideal smart grid requires significant investments in time, funding, and ongoing research. As the energy sector pushes forward in pursuit of a cleaner, more efficient, and connected power infrastructure, the complexity of smart grids continues to grow—especially as they incorporate countless interconnected devices and link to external networks, including the Internet. Understanding the cyber components and the broader implications of this highly integrated environment is critical.

The diverse range of hardware and software used in smart grid sensors fosters healthy competition in the U.S. technology market. However, this same diversity presents serious cybersecurity challenges. Without a unified security architecture overseeing the entire system, vulnerabilities can emerge across different platforms. Experts widely agree that while standards and frameworks provide important guidance, they alone cannot guarantee sufficient protection for such complex systems.

AI is increasingly seen as a transformative solution. Although still developing, AI—particularly technologies like deep learning—is already reshaping how utilities manage cybersecurity. AI holds strong promise in enhancing threat detection and response within smart grid environments, offering capabilities that traditional tools lack. Despite the existence of regulatory frameworks, creating and managing an effective security strategy for the U.S. smart grid remains a demanding task. This paper examines key trends, challenges, and emerging solutions in cybersecurity for critical smart grid infrastructure, focusing on the integration of big data and AI technologies. It also presents a comprehensive state-of-the-art review and proposes specific recommendations for establishing cybersecurity awareness programs tailored to the unique needs of the American energy sector.

References

J. Klaimi, R. Rahim-Amoud, L. Merghem-Boulahia, and A. Jrad, "A novel loss-based energy management approach for smart grids using multi-agent systems and intelligent storage systems," *Sustainable Cities and Society,* vol. 39, pp. 344-357, 2018/05/01/ 2018, doi: https://doi.org/10.1016/j.scs.2018.02.038.

K. N. Qureshi, R. Hussain, and G. Jeon, "A Distributed Software Defined Networking Model to Improve the Scalability and Quality of Services for Flexible Green Energy Internet for Smart Grid Systems," *Computers & Electrical Engineering,* vol. 84, p. 106634, 2020/06/01/ 2020, doi: https://doi.org/10.1016/j.compeleceng.2020.106634.

N. Chakraborty, A. Mondal, and S. Mondal, "Efficient Load Control Based Demand Side Management Schemes Towards a Smart Energy Grid System," *Sustainable Cities and Society,* vol. 59, p. 102175, 2020/08/01/ 2020, doi: https://doi.org/10.1016/j.scs.2020.102175.

K. K. N, I. G. V, L. Ravi, V. V, and S. V, "Improving security for wind energy systems in smart grid applications using digital protection technique," *Sustainable Cities and Society,* vol. 60, p. 102265, 2020/09/01/ 2020, doi: https://doi.org/10.1016/j.scs.2020.102265.

A. Chehri and H. T. Mouftah, "Service-oriented architecture for smart building energy management," in *2013 IEEE International Conference on Communications (ICC)*, 2013: IEEE, pp. 4099-4103.

A. Aloseel, H. He, C. Shaw, and M. A. Khan, "Analytical review of cybersecurity for embedded systems," *Ieee Access,* vol. 9, pp. 961-982, 2020.

C. Glenn, D. Sterbentz, and A. Wright, "Cyber threat and vulnerability analysis of the US electric sector," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2016.

A. Ferreira, P. Leitão, and P. Vrba, "Challenges of ICT and artificial intelligence in smart grids," in *2014 IEEE International Workshop on Intelligent Energy Systems (IWIES)*, 2014: IEEE, pp. 6-11.

H. Zhao, *Cyberspace & sovereignty*. World Scientific, 2022.

D. E. Mills, I. Izadgoshasb, and S. G. Pudney, "Smart city collaboration: A review and an agenda for establishing sustainable collaboration," *Sustainability,* vol. 13, no. 16, p. 9189, 2021.

G. Viale Pereira, C. M. Alexandra, L. T. J., P. Peter, and M. G. and Testa, "Increasing collaboration and participation in smart city governance: a cross-case analysis of smart city initiatives," *Information Technology for Development,* vol. 23, no. 3, pp. 526-553, 2017/07/03 2017, doi: 10.1080/02681102.2017.1353946.

D. Hoornweg and K. Pope, "Population predictions for the world’s largest cities in the 21st century," *Environment and urbanization,* vol. 29, no. 1, pp. 195-216, 2017.

J. R. Kenworthy, "Transport energy use and greenhouse gases in urban passengertransport systems: A study of 84 global cities," in *International sustainability conference*, 2003.

J. E. Rossebø, R. Wolthuis, F. Fransen, G. Björkman, and N. Medeiros, "An enhanced risk-assessment methodology for smart grids," *Computer,* vol. 50, no. 4, pp. 62-71, 2017.

H. Kang, S. Jung, M. Lee, and T. Hong, "How to better share energy towards a carbon-neutral city? A review on application strategies of battery energy storage system in city," *Renewable and Sustainable Energy Reviews,* vol. 157, p. 112113, 2022/04/01/ 2022, doi: https://doi.org/10.1016/j.rser.2022.112113.

L. Guo, M. Dong, K. Ota, J. Wu, and J. Li, "Event-oriented dynamic security service for demand response in smart grid employing mobile networks," *China Communications,* vol. 12, no. 12, pp. 63-75, 2015.

Y. Lopes *et al.*, "Vulnerabilities and threats in smart grid communication networks," in *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government*: IGI Global Scientific Publishing, 2021, pp. 1508-1535.

Z. Wenhua *et al.*, "Data security in smart devices: Advancement, constraints and future recommendations," *IET Networks,* vol. 12, no. 6, pp. 269-281, 2023.

M. K. Hasan, A. K. M. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications,* vol. 209, p. 103540, 2023/01/01/ 2023, doi: https://doi.org/10.1016/j.jnca.2022.103540.

M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, p. 107094, 2020/03/14/ 2020, doi: https://doi.org/10.1016/j.comnet.2019.107094.

Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering,* vol. 67, pp. 469-482, 2018/04/01/ 2018, doi: https://doi.org/10.1016/j.compeleceng.2018.01.015.

A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability,* vol. 13, no. 6, p. 3196, 2021.

A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment," *Journal of Advanced Research,* vol. 5, no. 4, pp. 481-489, 2014/07/01/ 2014, doi: https://doi.org/10.1016/j.jare.2013.12.005.

E. Avelar, L. Marques, D. dos Passos, R. Macedo, K. Dias, and M. Nogueira, "Interoperability issues on heterogeneous wireless communication for smart cities," *Computer Communications,* vol. 58, pp. 4-15, 2015/03/01/ 2015, doi: https://doi.org/10.1016/j.comcom.2014.07.005.

D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Computers & Security,* vol. 89, p. 101666, 2020/02/01/ 2020, doi: https://doi.org/10.1016/j.cose.2019.101666.

C. Bekara, "Security Issues and Challenges for the IoT-based Smart Grid," *Procedia Computer Science,* vol. 34, pp. 532-537, 2014/01/01/ 2014, doi: https://doi.org/10.1016/j.procs.2014.07.064.

C.-W. Tsai, C.-F. Lai, H.-C. Chao, and A. V. Vasilakos, "Big data analytics: a survey," *Journal of Big data,* vol. 2, pp. 1-32, 2015.

E. G. Dada, J. S. Bassi, H. Chiroma, S. i. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," *Heliyon,* vol. 5, no. 6, 2019.

A. S. Ali, S. Azad, and T. Khorshed, "Securing the smart grid: A machine learning approach," *Smart Grids: Opportunities, Developments, and Trends,* pp. 169-198, 2013.

M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Transactions on Smart Grid,* vol. 10, no. 5, pp. 5174-5185, 2018.

R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4930-4941, 2017.

S. Ahmadian, H. Malki, and Z. Han, "Cyber attacks on smart energy grids using generative adverserial networks," in *2018 IEEE global conference on signal and information processing (GlobalSIP)*, 2018: IEEE, pp. 942-946.

X. Li, J. Ma, Y. Zhu, and Y. Liu, "Extraction of abnormal points from on-line operation data of intelligent meter based on LSTM," in *2019 IEEE 9th annual international conference on CYBER technology in automation, control, and intelligent systems (CYBER)*, 2019: IEEE, pp. 586-591.

J. Moradi, H. Shahinzadeh, H. Nafisi, M. Marzband, and G. B. Gharehpetian, "Attributes of big data analytics for data-driven decision making in cyber-physical power systems," in *2020 14th international conference on protection and automation of power systems (IPAPS)*, 2019: IEEE, pp. 83-92.

H. do Nascimento Alves, N. G. Bretas, A. S. Bretas, and B.-H. Matthews, "Smart grids false data injection identification: a deep learning approach," in *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2019: IEEE, pp. 1-5.

Y. Zhang and J. Yan, "Domain-adversarial transfer learning for robust intrusion detection in the smart grid," in *2019 IEEE international conference on communications, control, and computing technologies for smart grids (SmartGridComm)*, 2019: IEEE, pp. 1-6.

R. Nawaz, R. Akhtar, M. A. Shahid, I. M. Qureshi, and M. H. Mahmood, "Machine learning based false data injection in smart grid," *International Journal of Electrical Power & Energy Systems,* vol. 130, p. 106819, 2021/09/01/ 2021, doi: https://doi.org/10.1016/j.ijepes.2021.106819.

M. Barati, "Faster than real-time prediction of disruptions in power grids using PMU: Gated recurrent unit approach," in *2019 IEEE power & energy society innovative smart grid technologies conference (ISGT)*, 2019: IEEE, pp. 1-5.

C. Hu, J. Yan, and C. Wang, "Advanced cyber-physical attack classification with extreme gradient boosting for smart transmission grids," in *2019 IEEE power & energy society general meeting (PESGM)*, 2019: IEEE, pp. 1-5.

M. I. Oozeer and S. Haykin, "Cognitive risk control for mitigating cyber-attack in smart grid," *IEEE Access,* vol. 7, pp. 125806-125826, 2019.

S. S. Noureen, S. B. Bayne, E. Shaffer, D. Porschet, and M. Berman, "Anomaly detection in cyber-physical system using logistic regression analysis," in *2019 IEEE texas power and energy conference (TPEC)*, 2019: IEEE, pp. 1-6.

M. R. C. Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE access,* vol. 8, pp. 19921-19933, 2020.

M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 8, pp. 2015-2030, 2018.

A. Amara korba and N. El Islem karabadji, "Smart grid energy fraud detection using SVM," in *2019 international conference on networking and advanced systems (ICNAS)*, 2019: IEEE, pp. 1-6.

B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 11, pp. 2415-2425, 2016.

K. Khanna, B. K. Panigrahi, and A. Joshi, "AI-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Generation, Transmission & Distribution,* vol. 12, no. 5, pp. 1052-1066, 2018.

T. Irita and T. Namerikawa, "Detection of replay attack on smart grid with code signal and bargaining game," in *2017 American Control Conference (ACC)*, 2017: IEEE, pp. 2112-2117.

R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access,* vol. 5, pp. 13787-13798, 2017.

H. Neema, P. Volgyesi, X. Koutsoukos, T. Roth, and C. Nguyen, "Online testbed for evaluating vulnerability of deep learning based power grid load forecasters," in *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2020: IEEE, pp. 1-6.

C. Pei, Y. Xiao, W. Liang, and X. Han, "Detecting false data injection attacks using canonical variate analysis in power grid," *IEEE Transactions on Network Science and Engineering,* vol. 8, no. 2, pp. 971-983, 2020.

W.-C. Hong, D.-R. Huang, C.-L. Chen, and J.-S. Lee, "Towards accurate and efficient classification of power system contingencies and cyber-attacks using recurrent neural networks," *IEEE Access,* vol. 8, pp. 123297-123309, 2020.

L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Evaluation of cyber-physical power systems in cascading failure: node vulnerability and systems connectivity," *IET Generation, Transmission & Distribution,* vol. 14, no. 7, pp. 1197-1206, 2020.

M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," *Computers & Security,* vol. 84, pp. 225-238, 2019/07/01/ 2019, doi: https://doi.org/10.1016/j.cose.2019.03.007.

P. V. Botvinkin, V. A. Kamaev, I. S. Nefedova, A. G. Finogeev, and E. A. Finogeev, "Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems," *arXiv preprint arXiv:1412.2387,* 2014.

D. Li, H. Guo, J. Zhou, L. Zhou, and J. W. Wong, "SCADAWall: A CPI-enabled firewall model for SCADA security," *Computers & Security,* vol. 80, pp. 134-154, 2019/01/01/ 2019, doi: https://doi.org/10.1016/j.cose.2018.10.002.

L. A. Maglaras, J. Jiang, and T. J. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems," *Journal of Information Security and Applications,* vol. 30, pp. 15-26, 2016/10/01/ 2016, doi: https://doi.org/10.1016/j.jisa.2016.04.002.

T. Cherifi and L. Hamami, "A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol," *International Journal of Critical Infrastructure Protection,* vol. 20, pp. 68-84, 2018/03/01/ 2018, doi: https://doi.org/10.1016/j.ijcip.2017.12.001.

V. H. Nguyen, Q. T. Tran, and Y. Besanger, "SCADA as a service approach for interoperability of micro-grid platforms," *Sustainable Energy, Grids and Networks,* vol. 8, pp. 26-36, 2016/12/01/ 2016, doi: https://doi.org/10.1016/j.segan.2016.08.001.

M. Ficco, M. Choraś, and R. Kozik, "Simulation platform for cyber-security and vulnerability analysis of critical infrastructures," *Journal of Computational Science,* vol. 22, pp. 179-186, 2017/09/01/ 2017, doi: https://doi.org/10.1016/j.jocs.2017.03.025.

P. T. C, K. G. Boroojeni, M. Hadi Amini, N. R. Sunitha, and S. S. Iyengar, "Key pre-distribution scheme with join leave support for SCADA systems," *International Journal of Critical Infrastructure Protection,* vol. 24, pp. 111-125, 2019/03/01/ 2019, doi: https://doi.org/10.1016/j.ijcip.2018.10.011.

N. R. Kumar, P. Mohanapriya, and M. Kalaiselvi, "Development of an attack-resistant and secure SCADA system using WSN, MANET, and Internet," *International Journal of Advanced Computer Research,* vol. 4, no. 2, p. 627, 2014.

L. Lee and P. Hu, "Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks," *International Journal of Electrical Power & Energy Systems,* vol. 111, pp. 182-190, 2019/10/01/ 2019, doi: https://doi.org/10.1016/j.ijepes.2019.03.062.

S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Applied Soft Computing,* vol. 71, pp. 66-77, 2018/10/01/ 2018, doi: https://doi.org/10.1016/j.asoc.2018.06.017.

S. S and P. W. D, "An enhanced optimization based algorithm for intrusion detection in SCADA network," *Computers & Security,* vol. 70, pp. 16-26, 2017/09/01/ 2017, doi: https://doi.org/10.1016/j.cose.2017.04.012.

Md Abdullah Al Mahmud, Nur Vanu, Sadia Islam Nilima, & Rakibul Hasan. (2021). Enhancing Customer Experience and Business Operations in E-Commerce Platforms through Big Data Analytics. *Journal of Business and Management Studies*, *3*(2), 288-295. https://doi.org/10.32996/jbms.2021.3.2.30.

Sadia Sharmin, & Rakibul Hasan. (2020). Financial Position Analysis of Bank Asia Limited for Small and Medium-Sized Businesses. *Journal of Economics, Finance and Accounting Studies* , *2*(2), 54-70. https://doi.org/10.32996/jefas.2020.2.2.6.