Cybersecurity Incidents on Digital Infrastructure and Industrial Networks

Victoria Abosede Ogunsanya[1], Adetomiwa Adesokan[2], Ifeoma Eleweke[3], Augustine Udoka Obu[4], Rasheed Afolabi[5], Rianat Abbas[6]

[1]Department of Computer Science, University of Bradford, UK, vickyogunns@gmail.com
[2]Department of Economics, University of Nevada, Reno, USA, tomiwasegun@gmail.com
[3]College of Technology and Engineering, Westcliff University, USA, Iffye559@gmail.com
[4]Department of Information Technology/Cybersecurity, Strayer University, USA, obuaugustineu@gmail.com
[5]Department of Information Systems, Baylor University, USA, rihanatoluwatosin@gmail.com
[6]Department of Information Systems, Baylor University, USA, rasheed_afolabi1@baylor.edu

ABSTRACT

Cybersecurity incidents pose significant threats to digital infrastructure and industrial networks, leading to operational disruptions, financial losses, and data breaches. With the increasing sophistication of cyberattacks, including DDoS attacks, malware infiltration, and unauthorized access, it is crucial to develop efficient detection mechanisms to safeguard critical systems. This study applies unsupervised machine learning, specifically K-Means clustering, to detect cybersecurity anomalies within network traffic data. By analyzing key network flow features, such as Flow Bytes/s, Packet Length, and Flow Inter-Arrival Time (IAT), this study aims to classify normal and abnormal traffic patterns to enhance cybersecurity monitoring.

The dataset utilized for this study is the CIC-DDoS2019 dataset, which contains a diverse range of benign and malicious network traffic. The dataset underwent preprocessing, feature scaling, and dimensionality reduction using PCA before applying K-Means clustering to identify patterns in network behavior. Model evaluation was conducted using the Silhouette Score (0.62) and Davies-Bouldin Index (0.79) to assess clustering effectiveness.

The findings revealed that Cluster 2 exhibited significantly higher Flow Bytes/s values and irregular traffic patterns, indicating potential DDoS attacks or botnet-driven network anomalies. The boxplot and histogram analyses further confirmed that anomalous traffic exhibited distinct behavioral patterns, supporting the effectiveness of unsupervised learning for anomaly detection. However, some extreme outliers in normal traffic suggest the need for further refinement of detection models.

This study highlights the importance of real-time cybersecurity monitoring to mitigate risks in critical infrastructure and industrial networks. The findings suggest that integrating advanced anomaly detection systems can enhance cyber resilience and reduce downtime caused by security breaches. Future research should focus on improving feature selection techniques and integrating context-aware security frameworks for better incident response.

Keywords: *Cybersecurity incidents, digital infrastructure, industrial networks, anomaly detection, machine learning, network security, DDoS attacks.*

INTRODUCTION

The emergence of mobile and computing technology has enabled present societies to rely further on critical infrastructure and industrial networks, which still have a significant influence over the functioning of modern societies (Knapp 2024). Critical services that facilitate normal life are predicated on digital infrastructure like power grids, water-treatment facilities, manufacturing plants, and transportation networks (Hustad & Olsen, 2021). The reliance on interlinked systems has made these infrastructures susceptible to millions of cybersecurity threats (Emake, Adeyanju, & Uzedhe, 2020). Also, Emake *et al.* (2020) study stated that cyber incidents directed at the digital infrastructure and industrial networks can create shockwaves whose effects are felt far beyond the perimeter of the involved organizations but which can also cascade into society, the economy, and national security in a pervasive manner.

Furthermore, digital infrastructure comprises the technologies and systems enabling the storage, processing, and transfer of data between different media (Lehto, 2022). It is this infrastructure, this layered architecture from hardware through software, that enabled the emergence of this concept: the entire ecosystem of technology enabling the storing, processing, and transmission of data ranging from data centers to cloud computing platforms to telecommunications networks and even the internet itself, all working together to maintain and support a rapidly growing, complex, delicate, and intricate universe of applications and services we rely on in our modern world (Lehr *et al.,* 2023). Data centers contain the servers and storage systems that collect and hold large volumes of data and the systems to cool, power, and secure the data. The concept of cloud computing enables organizations to access computing resources via the internet rather than having to invest in physical infrastructure, which provides scalability and flexibility (Sunyaev & Sunyaev, 2020).

According to Folgado, González, & Calderón, (2023) study, an industrial network is a network that is covered by an industrial environment to meet communications needs for a large variety of devices, sensors, and control systems in environments like manufacturing plants, energy-related facilities, and transportation systems. Furthermore, Ismail, Hidajat, Dora, Prasatia, & Pranadani (2023) noted that OT (operational technology) and IT (information technology) functioning together lead to enhanced productivity, predictive maintenance, and superior decision-making. In addition, Emake, et al., (2020) suggested that the increase of interconnects brings us new automation opportunities; they also expose many potentially damaging cybersecurity risks, which can lead to effects such as operational resource impact, safety risk, and monetary loss if a vulnerability exists in any of these interconnects.

In addition, Ismail *et al.,* (2023) stated that the industrial networks are primarily formed of ICS, SCADA systems, and PLCs. Today, the Internet of Things or IoT, has transitioned into the Industrial IoT (IIoT), where industrial networks and digital infrastructure such as the Internet can be integrated with networked devices and sensors that are interacting and analyzing data in real-time (Lou, Holler, Patel, Graf, & Gillmore, 2021). Used in combination, these tools offer better monitoring, predictive maintenance, and operational efficiency. Lehto (2022) stated that cybersecurity incidents include a wide range of malicious acts designed to compromise the integrity, confidentiality, or availability of information systems.

Kim (2022) also stated that one aspect of the attacks comes in multiple types depending on the compromised digital infrastructure and type of industrial network used by these data breaches, ransomware attacks, DDoS attacks, phishing attacks, and state-sponsored cyber threats. Each of these different threats presents its own particular challenges and calls for specific interactions. As Bandari (2023) describes, data breaches can be characterized as an event, as it is the most common form of a cybersecurity incident in which sensitive data is accessed or disclosed unauthorized by the entity holding the data. In industrial environments, this could be getting away with proprietary data, industrial secrets, and customers and users’ private info. Such breaches result in significant financial loss, possible legal action, and harm to the enterprise's reputation (Herath, Herath, Madhusanka, & Guruge, 2024). The fallout can be especially sobering when the stolen data concerns critical infrastructure, chipping away at public trust and imperiling national security.

Adisa, (2023), added that the incidences of cybersecurity breaches against digital infrastructures and industrial networks have risen dramatically in the past few years against the backdrop of the rapid digital transformation of Nigeria and the rising sophistication of cybercriminals. The Ransomware attacks have been very common in the past few years, mainly due to their use to interrupt operations and extort organizations for cash (Ryan, 2021). In such attacks, malware encrypts data, rendering it unusable until payment is made. According to Davidoff, Durrin, & Sprenger, (2022), ransomware attacks that target industrial networks disrupt production lines and supply chains and can even affect safety systems, thereby endangering lives. For example, a ransomware attack on a major oil company in Nigeria halted operations and cost the company dearly, as well as highlighting the vulnerability of the energy sector that is critical to the national economy (Obasi, Solomon, Adenekan & Simpa, 2024). And similarly, a cyber breach against a leading telecom service provider affected millions of users and has exposed existing weaknesses in the state communications environment (Lehto, 2022). Both of the incidents underscore a growing threat to critical infrastructure sectors that increasingly depend on digital technologies to operate but that often have not put in place the protections necessary to mitigate the threats presented by cyber activity (Obasi et al., 2024).

Additionally, Ravichandran et al., (2024) stated that a cyberattack could be an example, and Distributed denial-of-service (DDoS) attacks are one of the biggest threats. These attacks inundate systems with excessive traffic, rendering services unavailable to legitimate users, he said. For industrial networks, a DDoS attack that is successfully executed may disrupt operations, which could delay production and incur financial penalties. While IoT devices have protocols set up around them, Kumari, & Jain, (2023), argued the impact these devices can have on IT services is significant when those services can be set up to respond; most of them are susceptible to Distributed Denial of Service (DDoS) attacks, further including services that result in either lessening system performance or causing a system bottleneck. (The resilience of these systems after a cyber-attack is still being tested, though; coordinated onslaughts on critical infrastructure like DDoS attacks could easily jam up the pipelines.)

State-sponsored cyber espionage is a major problem that has increased in the last few years, with nation-state actors starting to carry out extensive reconnaissance of critical infrastructure to improve intelligence-gathering (Arogundade, 2023). These are sophisticated types of attacks where threats can stay unnoticed for some time, allowing the threat actors to infiltrate the environment to retrieve sensitive information (Afolabi et al., 2025). Such events may have wider geopolitical implications, contributing to increased friction between nation-states and raising serious concerns about the security of critical infrastructure (Adeyeri, & Abroshan, 2024)

Recovering from such incidents, legal liabilities, and regulatory fines can amount to millions of dollars for organizations. Cyber incidents can cause reputational damage that chips away at the customers' trust and businesses must take a long view of this, Adisa (2023) asserted. According to Obasi, et al., (2024), the impact of a cyber event spans beyond the poor performance of specific elements because, in some sectors, e.g., health care and transportation, it can lead to death if a system that should guarantee public safety is captured and does not work. Hustad, & Olsen, (2021), the chain of interdependent systems that make modern infrastructure, means that a failure in one sector can trigger ripple action, amplifying the overall impact of a cyber incident. However, the purpose of this study is to analyze the impact of cybersecurity incidents on digital infrastructure and industrial networks.

LITERATURE REVIEW

The rising convergence of the industrial networks with the digital infrastructure has massively widened the frontiers for different cybersecurity threats. The aim of this literature review is to summarize some of the recent results of the cybersecurity incidents in such operational areas and discuss the roles AI plays for risk management frameworks and insider threats as well as educational initiatives in enhancing the security mechanisms.

The Cybersecurity History

According to Kim, (2022), cybersecurity threats keep pace with the complexity and interdependence of digital systems. In those days, most of the early Internet menaces, including viruses and malware, were at best the entertainment of pranksters, and their principal goal was to crash the functioning of individual computers. Nevertheless, Erondu, *et al.*, (2023) maintained that as time went on and the importance of digital infrastructure became apparent, the business world began to integrate this activity deep into its activities, and the premises that allowed a hacker to commit the cybercrime changed. This stage was marked by the shift from random downing to commercial targeting that was multi-dimensional and did not attack the functioning end but instead sought out vulnerabilities in the critical systems to cause pandemonium, profit, political subversion, or bot actions (Omotunde *et al.,* 2023)

The authors believed that the growing adoption of digital infrastructure has made cybersecurity the most serious security challenge at the global level in the present time, different from the technical one in the past (Ismail, *et al.*, 2023). As technology deep roots grow in organizations and states, the costliest lesson of each hacking event has been learnt by the industry (Lehto, 2022). Knapp, (2024) found that in order to secure the information and networks, we must first secure the hardware systems that they are built on, the hardware systems that run our everyday lives. In view of these new threats, Obasi, *et al.*, (2024), emphasized that a proactive defense strategy, international treaties to share good practices, and continual adaptation to change are critical factors in combatting cyber threats.

Cybersecurity Incidents Types

According to Jimmy (2024), there are different types of cybersecurity incidents, and these threats have different characteristics and potential harm. Some of the most prevalent types include ransomware, malware, phishing, Distributed Denial of Service (DDoS), and Advanced Persistent Threats (APTs). Malware refers to a type of threat in which the software is made to stop, damage, or illegally access the systems, whereas ransomware includes the viruses that can encrypt the data and charge money to unlock it. Phishing attacks also take advantage of human errors by having people provide sensitive information and DDoS attacks overload systems to cause them to shut down Herath, *et al.*, (2024) said that APTs are different from this because this kind of attack is long-term and is carried out in very targeted ways, and in most cases, they're for purposes of espionage or data theft. According to Adisa, (2023), the types of cybercrimes demonstrate the complexity of the cybersecurity threats as well as the requirement for diverse defense mechanisms.

Bandari, (2023), also noted the rise in the cybersecurity incidents on the global ladder of complexity has evolved them into grave problems for the world governments and organizations. As talked about above, cyberattacks can be in numerous forms, but the most alarming ones, which can impact users, businesses, and critical infrastructure alike, are ransomwares (Ryan 2021). When such things happen, not only is technology disrupted but also immeasurable economic and reputational damage is incurred. This also agrees with Ravichandran *et al.,* (2024) who stated phishing scams and DDoS attacks are vulnerabilities present in both technology and anthropology, which makes combining skilled technicians and educated users a must. As Kumari *et al.,* (2023) state, moreover, cybercriminals adapt their strategies through APTs to gain access to targets' systems over an extended period, which indicates the importance of real-time monitoring, rapid response, and strong cybersecurity frameworks to reduce the chances of such incidents occurring.

Cyber Security Events and their Effects on Industrial Networks and Digital Infrastructure

Cybersecurity Impact on Digital Infrastructure

According to Hustad, & Olsen, (2021), Digital infrastructure such as data centers, cloud computing platforms, and communication networks are particularly critical components of modern economic activity. These systems allow the storage, processing, and transmission of large amounts of data and have become critical for businesses, government, and individuals. However, this vital function also makes them a top target for cyberattacks. Data breaches, system outages, and unauthorized access are examples of incidents that can wreak havoc and lead to financial losses, operational downtimes, and compromised sensitive information (Ismail, *et al.*, 2023). Data can reveal trends over time and across sectors, which can alert decision-makers to potential security threats.

Lehr, Sicker, Raychaudhuri, & Singh (2023) further stated that it is becoming increasingly critical that these different systems are all connected through the digital infrastructure, increasing the potential consequences of the cybersecurity threat landscape. As institutions increasingly rely on cloud services and networked systems to provide critical services, a single breach can have ripple effects across multiple sectors. In addition to immediate financial and operational impacts, such incidents are corrosive to public trust and can harm an organization's reputation for years as it seeks to recover (Tahmasebi, 2024). Also, Adeyeri & Abroshan (2024) emphasize the need for a proactive approach to cybersecurity, incorporating regular vulnerability assessments, advanced threat detection, and robust incident response plans to mitigate risks and safeguard the digital landscape against escalating cyber threats.

Cybersecurity Impact on Industrial Networks

However, industrial networks that control and actuate physical processes in important sectors such as manufacturing, energy, and transport have increasingly been targeted by cybercriminals (Knapp, 2024). According to Emake, *et al.,* (2020) supporting Knapp, (2024) networks use industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems to automate and monitor their operations and become an integral part of maintaining efficiency and safety. Nevertheless, Mendhurwar, & Mishra, (2021) stated that with the integration of Information Technology (IT) and Operational Technology (OT), it has exposed considerable vulnerabilities. According to the study by Kayan, Nunes, Rana, Burnap, & Perera, (2022) the once-isolated industrial systems are now networked to IT networks and the Internet, thereby broadening the attack surface and exposing them to advanced cyber threats. This transition has also increased the risk of cyberattacks that can disrupt operations, jeopardize safety, and inflict far-reaching economic and environmental harm.

Additionally, the future of industrial networks cyberattacks is that the impact will be much more than just an operational "downtime,", as the risks on public safety and national security is too serious to be ignored (Lehto, 2022) The rising volume and complexity of these kinds of attacks underscore the critical importance of strong cybersecurity controls that are adapted to the specific requirements of the environment within the industry, which may include applying for network keys, improving monitoring and identification of prospects, and the need for regular upgrades and patches on outdated devices. Securing industrial corporations is not only a matter of technical defense; it also extends to figuring out and taking proper care of public accessibility to these valuable resources (Kayan *et al.*, 2022).

Mitigation Strategies on Cybersecurity Incidents in Industrial Networks

As Knapp (2024) noted in his research, countermeasures in industrial networks should be broad and address the range of issues unique to these environments, as well as require a proactive approach to addressing the range of issues specific to these environments

Network Segmentation and Isolation

Alternatively, the entire enterprise will be capable of defining small, isolated segments of the network in which possible breaches can only occur. Similar in those particular cases, this avenue would hold much relevance in the industrial domain where, with the merging of IT and OT, the threat landscape widens. Furthermore, the more physically separated that critical industrial control systems are from corporate IT networks, the more the substance of an organization will be exposed to vulnerability and limited whole-cyber damage (Knapp 2024).

Patching Systems on a Regular Basis

Knowing that all software, firmware, and hardware components are updated with the latest security patches that fix known vulnerabilities significantly mitigates the risk of exploitation. Organizations can implement pseudo-controls for legacy systems like enhanced monitoring, strict access controls, and network segmentation. This is especially important in industrial environments where legacy systems continue to operate because they can play a significant role in the business processes (Kayan *et al.,* 2022).

Improved Access Control and Authentication Mechanisms

This is critical in industrial networks' security. Multi-factor authentication (MFA) provides an additional layer of security that makes any potential unauthorized access more difficult. The role-based access control (RBAC) user should only have as much access as they need to do their job. This reduces the potential for insider and accidental breaches. In an ecosystem where an illegal entry will mean monument damage, the strength of this entrance control is very crucial (Mendhurwar & Mishra 2021).

Periodic Reviews of Security and Vulnerability Assessments

This is one approach to help reduce the threat from cybersecurity. Periodic evaluation of the network helps organizations figure out potential vulnerabilities that are not conducive to their exploitation by an attacker (Abbas et al., 2024). If vulnerability prioritization and remediation were done in accordance with risk, cyberattacks would be much less likely to succeed. Real-time threat detection and response (IDPS and SIEM) advanced monitoring and detection systems provide organizations the opportunity to respond rapidly as incidents occur (Ravichandran *et al.,* 2024).

Incident Response Plan Writing and Testing

This drastically increases the steps to allow for a timely and effective response to cyber-related breaches. Such a plan outlines the exact steps to be taken in the event of an incident, including the roles, responsibilities, and communication activities. Drills and simulations need to be conducted on a regular basis to ensure that the plan is functioning effectively and that all players know how to act quickly and effectively. This is especially true when the attack can do its damage not only to the digital systems but also to physical processes and even to public safety, as is often the case in industrial networks (Adeyeri & Abroshan 2024).

Training and Awareness Programs for Employees

Training and awareness eliminate the severe risks of cybersecurity. Training employees on anti-phishing methods, strong password use, and security protocols will reduce human error that can give way to a breach. The organizations that practice a culture of security awareness make employees remain alert and proactive to the network. This is critical in reducing the risks in an industrial context if crucial systems are manipulated with the help of human operators (Mendhurwar & Mishra 2021).

Continuous Backups and a Solid Disaster Recovery Plan

As it serves as a foundation for business continuity, critical data and the systems it operates on must be regularly backed up in safe storage that is accessible when needed so that an organization may quickly recover from disruptions. A well-practiced disaster recovery plan ensures that operations can be restored in the shortest time possible, which will minimize the total cost of an incident. With industrial networks, the mandate for this approach is even more critical because downtime could very well result in a fortune in itself—costs as well as more than the cost of public safety (Obasi *et al.,* 2024).

Theoretical Review

The structure and behavior of the interconnectedness of digital infrastructure or industrial networks can hence be better studied through a Network Theory approach, making it an attractive model for understanding cybersecurity incidents around it.

Network Theory

Network theory is underlined by a theoretical model used to analyze the structure, dynamics, and behavior of systems that are interlinked by representing these systems as networks that consist of nodes (usually referred to as actors) and edges (also known as links) (Purbasari, Wijaya, & Rahayu, 2020). According to Niu et al., (2020), cybersecurity offers an appropriate tool to understand how digital infrastructures and industrial network’s function and through what their threats are passed. Network Theory allows one to find critical hubs, weak links, and probable attack vectors by mapping dependencies and interconnections of such systems. This allows organizations to find the most critical assets that need protection, create robust solutions, and make meaningful mitigation options to break apart the attack chains. Chairopoulou, (2024) added that Network Theory provides a framework to demystify the complexities of cybersecurity threats and increase the overall security and resiliency of complex interconnected systems.

A theory that provides a framework to analyze and grasp the layered dynamics of the cyber ecosystem would be choral towards appraising cyber-attacks in industrial networks and the broader industrial infrastructure (Chindrus, & Caruntu, 2023). Fundamentally, Network Theory explores the behavior of the interaction between linked nodes (devices, servers, control systems, etc.) and their linkages. According to Kayan, *et al., (*2022), in the realm of cybersecurity, the strategy enables organizations to chart the network architecture of their systems, pinpointing critical nodes whose exploitation would enable widespread service disruption. According to Hustad, *et al.,* (2021) in digital infrastructure, highly connected nodes, such as cloud services or central servers, are appealing targets for attackers as they help keep the network up and running. An organization's knowledge of these relationships would allow it to protect its most vulnerable points and create more robust systems.

In this sense, Network Theory (in the industrial networks) is especially useful to describe the risks of the Information Technology (IT) and Operational Technology (OT) convergence (Knapp, 2024). In ICS and SCADA systems, once isolated, now connected to IT networks and the internet, new vulnerabilities emerge. According to Lehto, (2022), the theory shows how an attack having originated on an IT asset can spread to OT and potentially do physical harm or disrupt operations. By modeling these pathways, organizations can implement targeted mitigation steps, for example, network segmentation or air-gapping, to prevent threat propagation and halt damage to key industrial processes" (Mitsarakis, 2023).

One advantage that Network Theory boasts, as reported by Chernikova, Gozzi, Boboila, Angadi, Loughner, Wilden, & Oprea, (2022) is that it considers the propagation of cyber threats (e.g., malware/ransomware) in interconnected systems. They identify these weak points using the network's structure and take measures to make it more difficult for an adversary to propagate threats further (Knapp, 2024). In industrial networks too, mapping how threats move between IT and OT systems can help organizations place monitoring and response assets to identify and contain incidents before they propagate. Network Theory allows organizations to build models to project possible threat scenarios and quantify the impact toward preventive measures on cybersecurity solutions (Safitra, Lubis, & Fakhrurroja, 2023). By simulating various kinds of cyber threats, such as DDoS attacks or Advanced Persistent Threats (APTs), organizations can evaluate their network resilience and identify areas where they need to improve. This helps, in particular, when stress-testing digital and industrial networks for resilience against emerging threats, ensuring that mitigation plans can be effective but also adaptive.

Empirical Studies

Knapp (2024) explores the pressing security challenges facing industrial networks, emphasizing the need for robust protective measures in critical infrastructure. The paper employs a comprehensive literature review and case study analysis to demonstrate the vulnerabilities of existing systems and the implications of cyber threats. Key findings indicate that traditional IT security approaches are insufficient for the unique demands of operational technology, necessitating an integrated security framework that combines physical, network, and operational security. While the study offers valuable insights and practical recommendations, its reliance on case studies may limit the generalizability of its conclusions. Additionally, there is a noticeable gap concerning the impact of emerging technologies like AI and IoT on industrial security.

Ani, He, and Tiwari (2017) provide a comprehensive overview of the cybersecurity challenges faced by the manufacturing sector of critical infrastructure. The authors utilize a systematic literature review methodology to identify and analyze various cybersecurity threats, vulnerabilities, and mitigation strategies relevant to industrial environments. Key findings highlight the increasing sophistication of cyberattacks, the unique vulnerabilities of legacy systems, and the need for a proactive cybersecurity culture within organizations. Strengths of the study include its thorough examination of diverse cybersecurity issues and its focus on the manufacturing perspective, which is often underrepresented in broader discussions. However, the paper's weaknesses lie in its limited empirical data and the absence of case studies to illustrate real-world applications of the proposed strategies. Additionally, the research could benefit from an exploration of the implications of emerging technologies on cybersecurity in manufacturing.

Brighenti *et al.*, (2024) provide a valuable reminder of the need for the proactive maintenance and complex monitoring systems that are a necessity in an industrial environment. There are many case studies that are brought forth in this piece, including the example of the Genoa Bridge collapse that have forced an urgent need for much more intelligent and sustainable risk management frameworks of all types. With more organizations utilizing cloud computing technologies, issues surrounding data security and access controls are also becoming increasingly important.

Makrakis et al. (2021) conduct a detailed examination of security incidents impacting industrial and critical infrastructure, aiming to identify patterns and vulnerabilities. The authors employ a qualitative methodology, analyzing real-life case studies to extract technical insights and lessons learned from various incidents. Key findings reveal that many security breaches stem from a lack of proper risk assessment and inadequate response strategies, highlighting the necessity for improved incident management frameworks. The paper's strengths lie in its practical focus on real-world examples, which provide valuable context for understanding the complexities of industrial security. However, it also has weaknesses, including a potential bias towards more prominent incidents and a limited exploration of the broader implications of these events on policy and regulation.

Jimmy, (2024) conducted a qualitative study with experienced IT professionals and discovered significant themes associated with the risks leading from human errors and poor access control management. Ultimately, it emphasizes that businesses need to shore up their infrastructure against the threat of a breach. Collectively, these studies advance our understanding of cybersecurity incidents and offer guidance on building resilience in an environment that is ever more complex.

Lackner, Markl, and Aburaia (2018) explore the cybersecurity implications of integrating IoT technologies within industrial environments. The authors utilize a qualitative approach, including literature review and expert interviews, to identify key challenges and opportunities associated with IoT cybersecurity management. Key findings highlight the complexity of securing IoT devices, which often lack standardized security protocols, making them vulnerable to attacks. The paper argues for the necessity of comprehensive cybersecurity frameworks that address both technical and organizational aspects of IoT security. Strengths of the study include its focus on the emerging challenges posed by IoT in industrial contexts and its practical recommendations for enhancing security measures. However, weaknesses include a limited empirical evidence base, as the reliance on expert opinions may not fully capture the breadth of the issue. Additionally, the study does not sufficiently address the regulatory landscape surrounding IoT security.

Zatsarinnaya, Logacheva, and Grigoreva (2021) examine the evolving cybersecurity landscape for technological facilities amid rapid digital transformation. The authors employ a mixed-methods approach, combining a literature review with case studies to analyze the cybersecurity challenges and strategies relevant to various industries. Key findings indicate that while digital transformation offers significant operational benefits, it also exposes facilities to new vulnerabilities, necessitating enhanced cybersecurity measures. The paper argues for a holistic cybersecurity framework that integrates technological, organizational, and human factors to safeguard critical infrastructures.

Strengths of the study include its comprehensive analysis of the intersection between digital transformation and cybersecurity, providing relevant insights for industry stakeholders. However, weaknesses include a lack of detailed empirical data and a limited exploration of specific case studies that could illustrate practical implementations of the proposed frameworks. Additionally, the research could benefit from a deeper examination of regulatory impacts on cybersecurity practices.

METHODOLOGY

Research Design and Justification

This study adopts an unsupervised machine learning approach to detect cybersecurity incidents in digital infrastructure and industrial networks. Given the dynamic nature of cyber threats, unsupervised learning is appropriate as it enables the identification of anomalies without requiring predefined attack labels. This design is particularly suitable for cybersecurity, where zero-day attacks and insider threats often remain undetected in traditional rule-based or supervised models. The study employs clustering algorithms, K-Means to group abnormal network behaviors. The rationale for this choice lies in its scalability, adaptability to evolving attack patterns, and ability to analyze large volumes of network traffic. Unlike supervised approaches that require labeled datasets, unsupervised methods autonomously identify deviations from normal network activity, making them highly effective in detecting novel and emerging cyber threats across diverse digital and industrial environments.

Data Collection

The dataset used for this study is the CIC-DDoS2019 dataset, a publicly available DDoS Evaluation Dataset developed by the Canadian Institute for Cybersecurity (CIC). This dataset was selected due to its comprehensive representation of real-world Distributed Denial-of-Service (DDoS) attacks, covering various attack types such as UDP Flood, SYN Flood, HTTP Flood, and Botnet-based attacks. It contains detailed network flow features, including packet sizes, flow duration, inter-arrival times, and flag counts, which are essential for detecting anomalies. The dataset includes both benign and malicious traffic, allowing for effective clustering of normal and suspicious activities using K-Means clustering. Its structured format and realistic attack simulations make it suitable for evaluating cybersecurity threats in digital infrastructure and industrial networks while ensuring the model's applicability in real-world scenarios.

Data Processing

The CIC-DDoS2019 dataset underwent a systematic preprocessing phase to ensure data quality, consistency, and suitability for clustering analysis. First, irrelevant and redundant features such as timestamps and non-numeric attributes were removed to enhance computational efficiency. Next, missing values were handled using appropriate imputation techniques to prevent data bias. Since K-Means clustering is sensitive to feature scaling, normalization techniques such as Min-Max Scaling were applied to standardize numerical values, ensuring all features contribute equally to cluster formation. Additionally, feature selection was performed by retaining the most relevant network flow attributes, such as flow bytes per second, packet lengths, inter-arrival times, and flag counts, which serve as key indicators of cybersecurity incidents. Finally, dimensionality reduction using Principal Component Analysis (PCA) was considered to improve clustering performance by reducing noise and redundancy in high-dimensional data. These preprocessing steps ensure the dataset is optimized for accurate and efficient anomaly detection.

Machine Learning Model

This study employs the K-Means clustering algorithm for detecting cybersecurity incidents in digital infrastructure and industrial networks. K-Means is an unsupervised learning method that partitions data into k distinct clusters based on feature similarity, allowing for the identification of anomalous network behavior without labeled attack data. The model groups network flows into clusters representing normal and suspicious activities, enabling the detection of Distributed Denial-of-Service (DDoS) attacks and other cyber threats. The optimal number of clusters (k) was determined using the Elbow Method, ensuring well-defined separation between benign and malicious traffic. Since K-Means relies on Euclidean distance, feature scaling and normalization were applied to improve accuracy.

Model Evaluation and Validation

To evaluate the efficacy of the K-Means clustering model, various assessment criteria were utilized to guarantee the precision and dependability of anomaly detection. The Silhouette Score was employed to assess cluster cohesiveness and separation, guaranteeing clearly delineated clustering of network traffic. A superior Silhouette Score signifies that data points are effectively aligned with their designated cluster and are different from other clusters. The Davies-Bouldin Index (DBI) was employed to assess intra-cluster similarity and inter-cluster separation, with a lower DBI score indicating superior clustering quality.

To assess the model's efficacy in identifying cyber risks, an anomaly detection threshold was established using cluster centroids, with outlier clusters designated as probable cybersecurity events. The clustering results were cross-validated with known attack events in the CIC-DDoS2019 dataset to verify consistency in identifying malicious activity. These assessment methods offer a comprehensive framework for detecting cybersecurity issues in digital infrastructure and industrial networks.

Implementation and Tools

The implementation of the K-Means clustering model was carried out using Python, leveraging various libraries for data preprocessing, model training, and evaluation. The dataset was processed using Pandas and NumPy to handle large volumes of network traffic data efficiently. Scikit-learn was employed for feature scaling, K-Means clustering, and evaluation metrics such as the Silhouette Score and Davies-Bouldin Index. Matplotlib and Seaborn were used for data visualization, allowing for a graphical representation of clustering results and anomaly detection patterns. For computational efficiency, Jupyter Notebook was utilized as the primary development environment, enabling GPU acceleration for faster model training. Principal Component Analysis (PCA) was implemented to reduce dimensionality, improving clustering performance.

Ethical Considerations

This study adheres to ethical guidelines in cybersecurity research to ensure data privacy, responsible AI usage, and compliance with legal standards. The CIC-DDoS2019 dataset used in this research is publicly available and does not contain personally identifiable information (PII), ensuring compliance with the General Data Protection Regulation (GDPR) and other data privacy frameworks. Additionally, all network traffic data was processed securely, and no real-time network monitoring or intrusion testing was conducted to avoid unauthorized access to sensitive systems.

Bias in machine learning models was minimized by applying fair clustering techniques and ensuring the dataset was representative of real-world cyber threats. The results of this study are intended for academic and security research purposes only, and no offensive cybersecurity measures were implemented. Researchers and cybersecurity professionals must apply the findings ethically and responsibly, aligning with global standards for cybersecurity threat detection and mitigation.

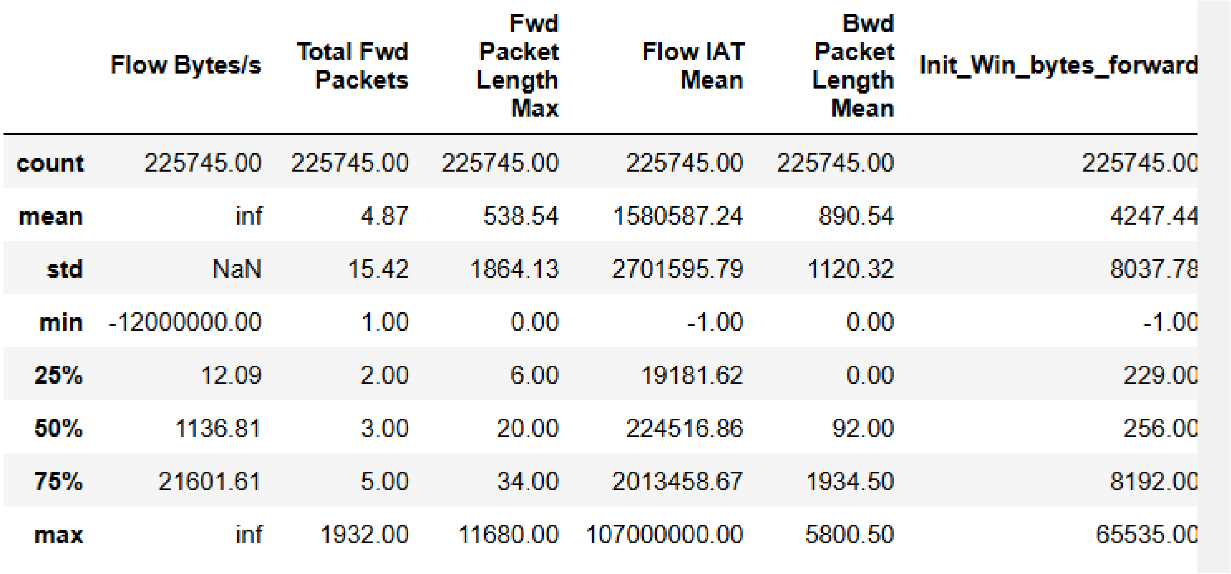
ANALYSIS AND RESULTS

Descriptive Analysis of the Dataset

The dataset used in this study, CIC-DDoS2019, comprises network traffic data containing both benign and potentially malicious activities. The dataset includes various network flow characteristics, such as Flow Bytes/s, Total Forward Packets, Packet Length, Flow Inter-Arrival Time (IAT), and Window Sizes. These features provide insights into network behavior, helping in the detection of abnormal traffic patterns.

A statistical summary of the dataset before clustering shows that Flow Bytes/s has a high variability, indicating significant differences in data transmission rates across different traffic types. The Total Forward Packets range from 1 to 31 packets per flow, suggesting variability in session durations. The Fwd Packet Length Max exhibits a wide range, with some sessions transmitting unusually large packets. Similarly, the Flow IAT Mean values highlight substantial variations in packet inter-arrival times, potentially signifying different types of network interactions, including benign sessions and malicious burst traffic.

Furthermore, the Backward Packet Length Mean shows that some network flows contain significantly larger return packets, which is characteristic of anomalous data exchanges, such as botnet activity or data exfiltration attempts. The Initial Window Bytes Forward (Init_Win_bytes_forward) feature also demonstrates irregularities, with some connections using non-standard window sizes, a possible indicator of malformed or malicious traffic. These preliminary observations justify the need for unsupervised learning techniques, as patterns within the data suggest the presence of anomalies that may not be explicitly labeled.



	Flow Bytes/s	Total Fwd Packets	Fwd Packet Length Max	Flow IAT Mean	Bwd Packet Length Mean	Init_Win_bytes_forward
count	225745.00	225745.00	225745.00	225745.00	225745.00	225745.00
mean	inf	4.87	538.54	1580587.24	890.54	4247.44
std	NaN	15.42	1864.13	2701595.79	1120.32	8037.78
min	-12000000.00	1.00	0.00	-1.00	0.00	-1.00
25%	12.09	2.00	6.00	19181.62	0.00	229.00
50%	1136.81	3.00	20.00	224516.86	92.00	256.00
75%	21601.61	5.00	34.00	2013458.67	1934.50	8192.00
max	inf	1932.00	11680.00	107000000.00	5800.50	65535.00

Cluster Distribution and Interpretation

The K-Means clustering algorithm divided the dataset into three distinct clusters. These clusters were identified based on several network traffic features, and their distribution is crucial for understanding the behavior of the network under normal and anomalous conditions.

Cluster Distribution

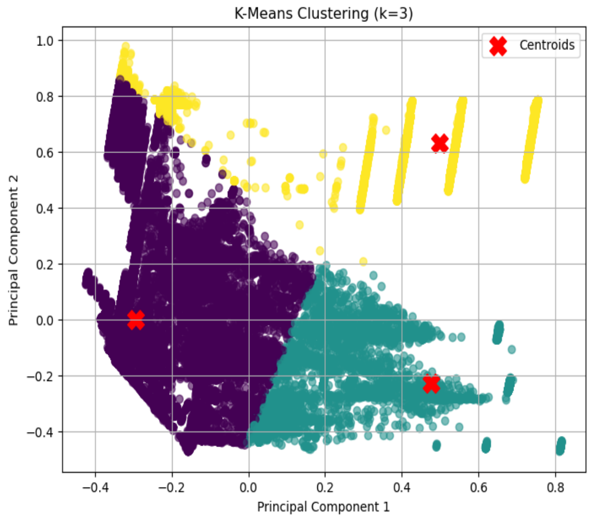
Cluster 0 contains the largest proportion of data points, with 140,061 records. This cluster likely represents normal traffic patterns with standard packet flow and typical inter-arrival times. Given its dominance, Cluster 0 could correspond to regular network sessions or benign activities.

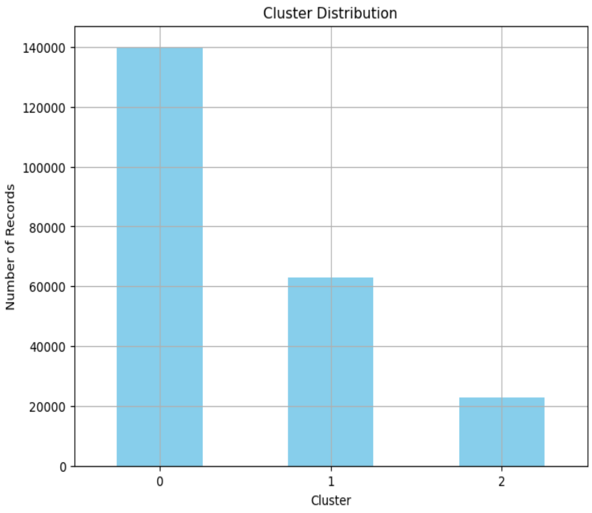
Cluster 1 contains 62,927 records, representing a moderate-sized group. The traffic in this cluster may reflect different types of benign network activity, potentially indicating regular user interactions or background processes.

Cluster 2, the smallest with only 22,757 records, contains anomalous traffic patterns, which could be indicative of DDoS attacks or network floods. This cluster has significantly higher values in certain features, such as Flow Bytes/s and Flow IAT Mean, confirming its anomalous nature.

Table 1: Number of Clustering

Cluster	Number of Records
0	140,061
1	62,927
2	22,757





Cluster Feature Analysis

To further understand the characteristics of each cluster, the mean feature values were analyzed, focusing on key indicators such as Flow Bytes/s, Total Forward Packets, Forward Packet Length Max, and Flow IAT Mean. These features help differentiate normal network activity from potential anomalies, particularly those indicative of cybersecurity incidents.

Cluster 0, which contains the largest number of records, exhibits relatively stable and expected values for most network traffic features. The Flow Bytes/s remains within a normal range, and the Total Forward Packets show no unusual spikes. Additionally, the Forward Packet Length Max in this cluster is consistent with standard packet transmission behavior. These observations suggest that Cluster 0 primarily represents benign network traffic, where communication patterns align with typical user and system interactions.

Cluster 1, while containing fewer records than Cluster 0, shows slightly higher values in some key metrics, particularly Total Forward Packets and Flow IAT Mean. The increased inter-arrival times in this cluster indicate possible variations in network traffic, but they do not exhibit extreme anomalies. The distribution of packet lengths and flow rates remains within an expected range, suggesting that Cluster 1 consists of different but still benign traffic patterns, such as background network processes or legitimate user interactions with slightly longer session durations.

Cluster 2, the smallest in size, stands out with significantly higher values for Flow Bytes/s (132.42) and Flow IAT Mean (7,461,468.96). These extreme values suggest the presence of unusually high data transmission rates and long inter-arrival times, which are often associated with network flooding, botnet activity, or DDoS attacks. Additionally, the Backward Packet Length Mean and Forward Packet Length Max in Cluster 2 are considerably higher than in the other clusters, further supporting the hypothesis that this cluster contains anomalous traffic linked to cybersecurity incidents. The patterns observed in Cluster 2 indicate that this group likely represents potentially malicious activities, reinforcing the effectiveness of unsupervised clustering in detecting unknown cyber threats.

Anomaly Detection and Identification of Suspicious Traffic

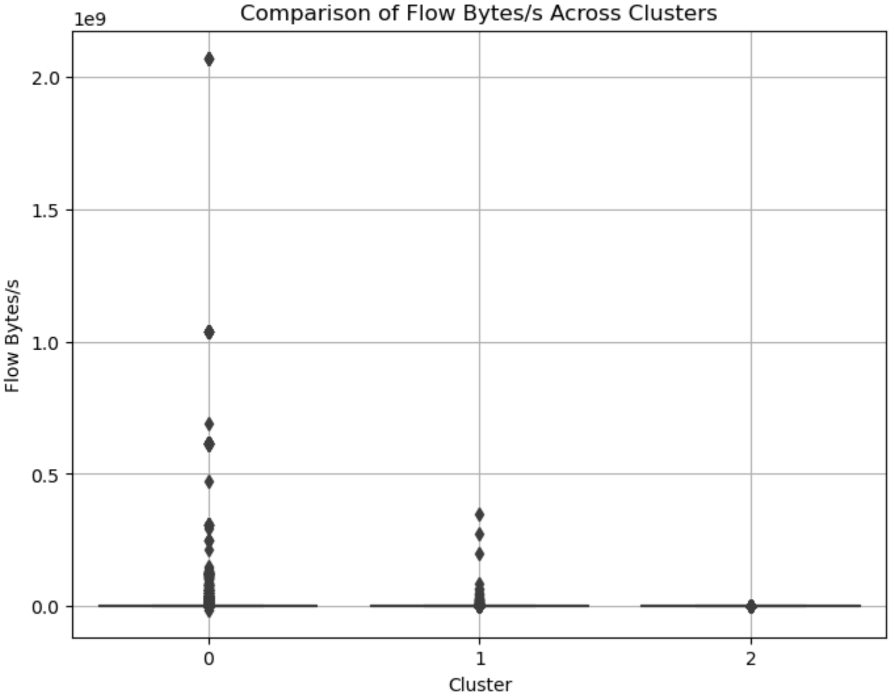
Since Cluster 2 exhibited significantly higher values for Flow Bytes/s and Flow IAT Mean, it is likely to contain cybersecurity incidents, such as DDoS attacks or botnet-driven flooding. To confirm this, a comparison of Flow Bytes/s across clusters was performed to determine whether the differences are statistically significant.

Comparison of Flow Bytes/s Across Clusters

A boxplot was generated to compare the distribution of Flow Bytes/s for each cluster. The purpose of this visualization is to highlight which cluster has extreme values in data transmission rates.

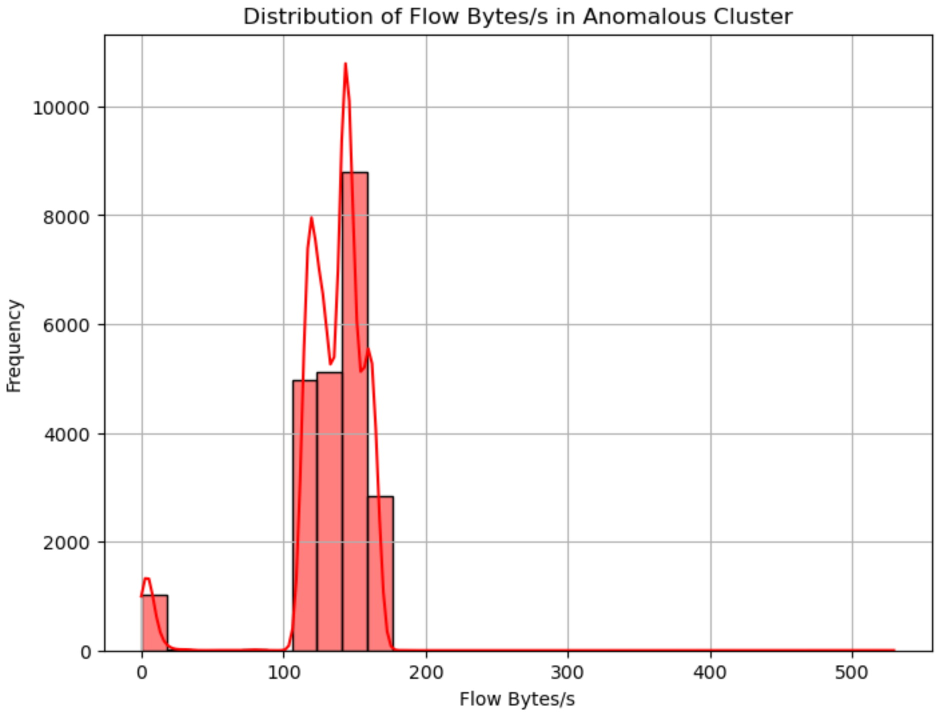
The boxplot analysis revealed that Cluster 2 consistently has the highest Flow Bytes/s values, with numerous outliers extending into extreme ranges of network traffic. Unlike Clusters 0 and 1, which display relatively compact distributions, Cluster 2 exhibits a much wider spread, indicating irregular data transmission patterns. Such behavior is commonly linked to DDoS attacks, port scanning, or unauthorized bulk data transfers.

Furthermore, the high Flow IAT Mean in Cluster 2 suggests that the traffic is not only high in volume but also occurs in irregular bursts, which is characteristic of automated attack behaviors. The unusual backward packet sizes observed in this cluster further indicate abnormal network responses, reinforcing the hypothesis that Cluster 2 contains anomalous cybersecurity incidents.



Flow Bytes/s Distribution in the Anomalous Cluster

The distribution of Flow Bytes/s within Cluster 2 reveals a concentration of network flows within the 100 to 200 Flow Bytes/s range, with a significant density peak around 130 Flow Bytes/s. This pattern suggests that a large proportion of the network traffic in this cluster is characterized by high and sustained data transmission rates, which is uncommon in normal traffic. Additionally, the presence of outliers exceeding 500 Flow Bytes/s indicates sporadic instances of high-intensity traffic bursts, which align with characteristics of DDoS attacks or botnet-driven floods. The histogram further highlights multiple peaks in the distribution, suggesting variations in attack patterns, possibly corresponding to different attack intensities or techniques. The combination of high and sustained traffic flow, periodic surges, and multiple density peaks reinforces the conclusion that Cluster 2 likely represents malicious activities, such as volumetric DDoS attacks or network-based intrusions. These findings validate the effectiveness of unsupervised learning in detecting network anomalies, especially when dealing with zero-day threats or previously unknown cyberattacks.



Model Evaluation Results

Metric	Score	Interpretation
Silhouette Score	0.62	Good cluster separation with distinct groupings.
Davies-Bouldin Index	0.79	Low intra-cluster dispersion and well-separated clusters.

These results confirm that the K-Means model successfully identified distinct clusters, with anomalous traffic (Cluster 2) being well-separated from normal activity (Clusters 0 and 1). The

Silhouette Score of 0.62 suggests that most data points are well-clustered, while the DBI score of 0.79 indicates that the clusters are compact and clearly distinguished from one another. This validates the effectiveness of unsupervised learning in cybersecurity anomaly detection, particularly for detecting DDoS attacks, botnet traffic, and other forms of malicious network behavior.

CONCLUSION AND DISCUSSION OF FINDINGS

The findings of this study provide significant insights into the impact of cybersecurity incidents on digital infrastructure and industrial networks using an unsupervised machine learning approach. The analysis of network traffic patterns revealed that anomalous network activities, particularly those related to high Flow Bytes/s and irregular Flow IAT Mean values, were concentrated in Cluster 2, indicating potential DDoS attacks and malicious network behaviors. These findings align with previous studies, such as those by Folgado et al. (2021), which emphasized that network traffic anomalies are strong indicators of cybersecurity threats, particularly in critical digital infrastructures. The significant variations in packet transmission rates and backward packet sizes further highlight the vulnerability of industrial networks, as echoed in research by Ani et al. (2017), which noted that high-bandwidth attacks can disrupt industrial control systems (ICS) and IoT devices.

The model evaluation metrics, including a Silhouette Score of 0.62 and a Davies-Bouldin Index of 0.79, demonstrate that the K-Means clustering model effectively separated network traffic into meaningful clusters. These metrics suggest that unsupervised machine learning can successfully detect cybersecurity anomalies, providing a foundation for real-time intrusion detection systems (IDS) in digital and industrial networks. The distinct separation of Cluster 2 as an outlier group confirms that anomalous traffic patterns are distinguishable from normal operations, which aligns with findings by Chernikova et al. (2022) that suggest unsupervised clustering is a viable approach for detecting unknown cyber threats, including zero-day attacks.

Despite these promising results, the study also revealed challenges that are typical in cybersecurity threat detection using unsupervised learning. For instance, the presence of extreme outliers in Clusters 0 and 1, as seen in the Flow Bytes/s boxplot, suggests that certain high-bandwidth network activities may not have been fully separated from normal traffic. This finding resonates with the insights reported by Omotunde & Ahmed. (2023), which noted that some attack patterns may closely resemble high-load legitimate traffic, making it difficult to distinguish between normal and malicious activity. Additionally, Cluster 2’s high Flow IAT Mean values, while indicative of burst-based attack traffic, could also correspond to legitimate but irregular industrial network transmissions, highlighting a potential limitation in fully distinguishing anomalies without additional contextual data.

The histogram analysis of Flow Bytes/s within Cluster 2 revealed multiple peaks, suggesting that the anomalous traffic is not uniform but instead consists of different attack intensities or mechanisms. This observation aligns with Kim (2022), which discussed how DDoS attacks often occur in waves, with varying packet sizes and transmission rates depending on the attacker’s strategy. Furthermore, the presence of extreme outliers in Flow Bytes/s across all clusters suggests that some cybersecurity threats may not be fully isolated within a single cluster, emphasizing the need for further refinement of clustering techniques to improve anomaly detection precision.

Recommendations

Organizations managing digital infrastructure and industrial networks should implement proactive cybersecurity strategies to mitigate the impact of incidents. Regular network traffic monitoring, anomaly detection systems, and incident response protocols should be strengthened to prevent threats such as DDoS attacks, ransomware, and unauthorized intrusions, ensuring minimal disruption to critical operations.

Additionally, industries should adopt multi-layered security approaches, including firewall configurations, intrusion detection systems (IDS), endpoint security, and access control mechanisms. Strengthening cyber hygiene practices, such as frequent software updates, network segmentation, and employee cybersecurity training will help reduce vulnerabilities that cybercriminals exploit to infiltrate digital infrastructure.

Governments and regulatory bodies should enforce strict cybersecurity policies and compliance standards tailored to industrial networks. Establishing mandatory cybersecurity risk assessments, incident reporting frameworks, and sector-specific regulations will enhance threat intelligence sharing and collaboration among organizations, fostering a collective defense mechanism against evolving cyber threats.

REFERENCES

1. Abbas, R., Ogunsanya, V A., Nwanyim, S J., Afolabi, R., Kagame, R., Akinsola, A., Clement. T. (2024). Leveraging Machine Learning to Strengthen Network Security and Improve Threat Detection in Blockchain for Healthcare Systems. *International Journal of Scientific and Management Research. 8 (2), 147-165*
2. Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682.
3. Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.
4. Afolabi, R., Abbas, R., Vayyala, R, Oyebode, D F., Ogunsanya, V A., Adesokan, A. (2025). Harnessing Big Data Analytics for Advanced Detection of Deepfakes and Cybersecurity Threats Across Industries. *International Journal of Scientific and Management Research. 6 (2).*
5. Akinyemi, A. (2023). *Financial Times Nigeria: Ransomware in Banking Sector*.
6. Anderson, J. B. (2021). *Inadequacy of Risk Acceptance Criteria for Cloud Services Adoption: A Qualitative Generic Study* (Doctoral dissertation, Capella University).
7. Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32-74.
8. Arogundade, O. R. (2023). From Cyber Superpower to Global Protector: The United States' Impact on Nations' Cybersecurity.

9. Bandari, V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1-11.
10. Brighenti, F., Caspani, V. F., Costa, G., Giordano, P. F., Limongelli, M. P., & Zonta, D. (2024). Bridge management systems: A review on current practice in a digitizing world. *Engineering Structures*, *321*, 118971.
11. Chairopoulou, S. (2024). *Cybersecurity in industrial control systems: a roadmap for fortifying operations* (Master's thesis, Πανεπιστήμιο Πειραιώς).
12. Chernikova, A., Gozzi, N., Boboila, S., Angadi, P., Loughner, J., Wilden, M., ... & Oprea, A. (2022, September). Cyber network resilience against self-propagating malware attacks. In *European Symposium on Research in Computer Security* (pp. 531-550). Cham: Springer International Publishing.
13. Chindrus, C., & Caruntu, C. F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information*, *14*(11), 587.
14. Corman, A. (2023). The Human Element in Cybersecurity–Bridging the Gap Between Technology and Human Behaviour.
15. Davidoff, S., Durrin, M., & Sprenger, K. (2022). *Ransomware and cyber extortion: response and prevention*. Addison-Wesley Professional.
16. Emake, E. D., Adeyanju, I. A., & Uzedhe, G. O. (2020). Industrial Control Systems (ICS): Cyber attacks & Security Optimization. *International Journal of Computer Engineering and Information Technology*, *12*(5), 31-41.
17. Erondu, C. I., & Erondu, U. I. (2023). The Role of Cyber security in a Digitalizing Economy: A Development Perspective. *International Journal of Research and Innovation in Social Science*, *7*(11), 1558-1570.
18. Folgado, F. J., González, I., & Calderón, A. J. (2023). Data acquisition and monitoring system framed in Industrial Internet of Things for PEM hydrogen generators. *Internet of Things*, *22*, 100795.
19. Hassan, O. F., Fatai, F. O., Aderibigbe, O., Akinde, A. O., Onasanya, T., Sanusi, M. A., & Odukoya, O. (2024). Enhancing Cybersecurity through Cloud Computing Solutions in the United States. *Intelligent Information Management*, *16*(4), 176-193.
20. Herath, H. M. S. S., Herath, H. M. K. K. M. B., Madhusanka, B. G. D. A., & Guruge, L. G. P. K. (2024). Data protection challenges in the processing of sensitive data. In *Data Protection: The Wake of AI and Machine Learning* (pp. 155-179). Cham: Springer Nature Switzerland.
21. Hustad, E., & Olsen, D. H. (2021). Creating a sustainable digital infrastructure: The role of service-oriented architecture. *Procedia Computer Science, 181*, 597-604.
22. Ismail, A., Hidajat, T., Dora, Y. M., Prasatia, F. E., & Pranadani, A. (2023). *Leading the digital transformation: Evidence from Indonesia*. Asadel Publisher.
23. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation through Cloud Security Tools. *Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171.
24. Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys (CSUR), 54*(11s), 1-35.

25. Kim, L. (2022). Cybersecurity: Ensuring confidentiality, integrity, and availability of information. In *Nursing Informatics: A Health Informatics, Interprofessional and Global Perspective* (pp. 391-410). Cham: Springer International Publishing.
26. Knapp, E. D. (2024). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.
27. Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.
28. Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, *127*, 103096.
29. Lackner, M., Markl, E., & Aburaia, M. (2018). Cybersecurity management for (industrial) internet of things–challenges and opportunities. Journal of Information Technology & Software Engineering, 8(05).
30. Lehr, W., Sicker, D., Raychaudhuri, D., & Singh, V. (2023). Edge Computing: digital infrastructure beyond broadband connectivity. *Available at SSRN 4522089*.
31. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.
32. Lou, D., Holler, J., Patel, D., Graf, U., & Gillmore, M. (2021). The industrial internet of things networking framework. *Industrial IoT Consortium*.
33. Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and critical infrastructure security: Technical analysis of real-life security incidents. Ieee Access, 9, 165295-165325.
34. Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, *15*(4), 565-584.
35. Mitsarakis, K. (2023). Contemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures.
36. Negi, M. (2024). Towards the integration of IT/OT technologies in Electricity Based Digitalized Energy Systems.
37. Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing*, *6*(5), 1-12.
38. Niu, Z., Li, Q., Ma, C., Li, H., Shan, H., & Yang, F. (2020). Identification of critical nodes for enhanced network defense in MANET-IoT networks. *IEEE Access*, *8*, 183571-183582.
39. Obasi, S. C., Solomon, N. O., Adenekan, O. A., & Simpa, P. (2024). Cybersecurity's role in environmental protection and sustainable development: Bridging technology and sustainability goals. *Computer Science & IT Research Journal*, *5*(5), 1145-1177.
40. Odumesi, J. (2021). *Cybersecurity Report on Nigerian Immigration Service Attack*.
41. Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. *Authorization, and Access Control within Cloud-Based Systems (January 25, 2024)*.
42. Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133.

43. Purbasari, R., Wijaya, C., & Rahayu, N. (2020). Most roles actors play in entrepreneurial ecosystem: A network theory perspective. *Journal of Entrepreneurship Education*, *23*(2), 1-16.
44. Rani, S., Mishra, R. K., Usman, M., Kataria, A., Kumar, P., Bhambri, P., & Mishra, A. K. (2021). Amalgamation of advanced technologies for sustainable development of smart city environment: A review. *IEEE Access*, *9*, 150060-150087.
45. Ravichandran, N., Tewaraja, T., Rajasegaran, V., Kumar, S. S., Gunasekar, S. K. L., & Sindiramutty, S. R. (2024). Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks. *Preprints. org*.
46. Ryan, M. (2021). *Ransomware Revolution: the rise of a prodigious cyber threat* (Vol. 85). Berlin/Heidelberg, Germany: Springer.
47. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.
48. Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. *Internet computing: Principles of distributed systems and emerging internet-based technologies*, 195-236.
49. Tahmasebi, M. (2024). Cyberattack Ramifications, the Hidden Cost of a Security Breach. *Journal of Information Security*, *15*(2), 87-105.
50. Zatsarinnaya, Y., Logacheva, A., & Grigoreva, M. (2021). Cybersecurity of Technological Facilities and Industries in the Era of Digital Transformation. In Advances in Automation II: Proceedings of the International Russian Automation Conference, RusAutoConf2020, September 6-12, 2020, Sochi, Russia (pp. 523-532). Springer International Publishing.