Journal of Information Systems Engineering and Management
2025, 10(19s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Navigating Cybersecurity Risks in Industry 4.0: Challenges, Threats, and Defense Strategies

Bhoopendra Singh[1], Brijesh Kumar[2]
1 Ph.D Research Scholar, Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, INDIA
[2] Prof. (Dr.) Brijesh Kumar, Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, INDIA

ARTICLE INFO

Received: 20 Dec 2024

Revised: 30 Jan 2025

Accepted: 15 Feb 2025

ABSTRACT

The rise of the Fourth Industrial Revolution, also known as Industry 4.0, has brought high-end technologies in industrial deployments like computer vision, big data analytics, and the Internet of Things (IoT). These advancements push the envelope for computing, but they come with security consequences that can shape an entirely new set of attack surfaces. This study addresses and investigates existing research and reports on the cybersecurity domain in Industry 4.0. We presented a systematic review of the academic literature, conference proceedings, and related observation studies characterizing cybersecurity risks and defenses. The study highlights the major cybersecurity threats in Industry 4.0, such as data security and privacy, as well as the overall security of the network and system reliability. The paper also outlines different approaches that can be undertaken to reduce these threats, including encryption, control access mechanisms, and network segmentation. The analysis part interprets the results, translates them to get some significant conclusions, and provides practical recommendations in terms of future research and implementation.

Keywords: Cyber Security; Encryption; Industry 4.0; Challenges; Mitigation Strategies; Data Analysis; Access Control; Network Segmentation

INTRODUCTION

This fourth industrialized society is referred to as the Fourth Industrial Revolution or Industry 4.0, which is characterized by the integration of various technologies into industrial practices. Such technologies include artificial intelligence (AI), big data analytics, and the Internet of Things (IoT) [1]. The application of these technologies is bound to change the landscape of manufacturing and industrial processes, increasing efficiency, flexibility, and responsiveness to changing customer needs. But as their use grows, new cybersecurity vulnerabilities need to be tackled. Industrial sector 4.0 people have lots of new - you will know that automation and monitoring by using the internet are not more local machines connected to the firm offline. Protecting information, systems, and networks is paramount for the trust, safety, and privacy of the industrial process [1]. Therefore, it is essential to recognize the cybersecurity challenges that Industry 4.0 faces and to evaluate the strategies used to mitigate these risks. The aim of this paper is, therefore, to present an extensive review of existing studies on the cybersecurity risks and mitigation techniques in Industry 4.0. It aims to identify the main cybersecurity challenges to Industry 4.0 and analyze the initiatives that are already in place to counter them. Moreover, by bringing together the findings of this paper, we aimed to establish a foundation for further research and serve as a guide to Industry 4.0 cybersecurity-related developments.

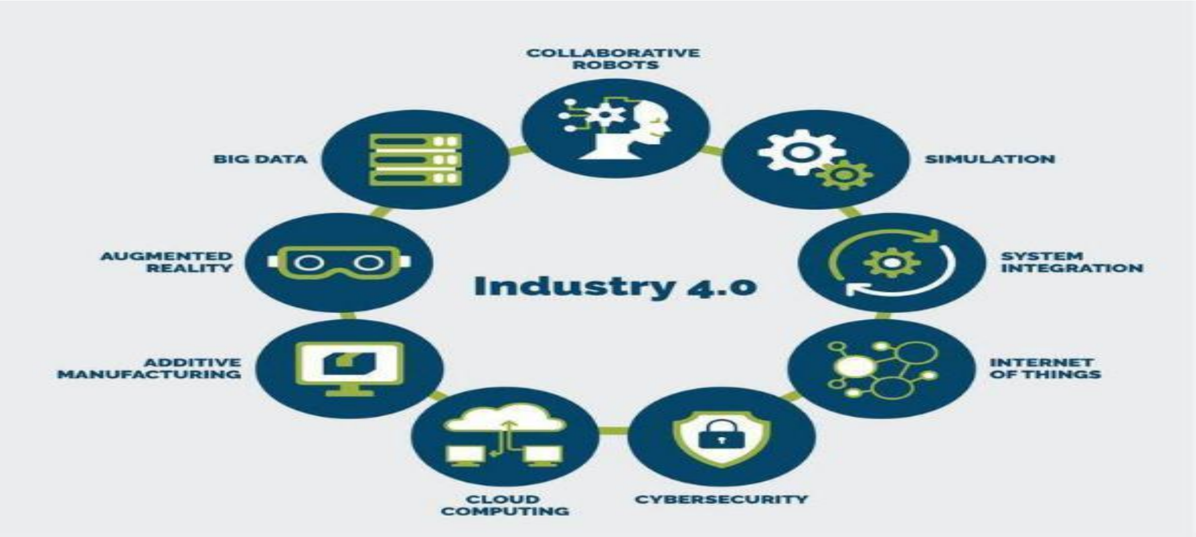

Figure 1. Technologies in Industry 4.0[16]

LITERATURE REVIEW

This also applies to recent studies on Industry 4.0 about cybersecurity, which highlight its challenges and complexities, and the existing strategies for security threat mitigation. Commonly, research findings highlight the increasing demand for improved security measures and risk mitigation strategies, as the adoption of sophisticated technologies introduces new vulnerabilities, putting critical infrastructure and sensitive data at increased risk.

Data privacy and security were made one of the main concerns in the literature. On one hand, Industry 4.0 technologies create and process considerable amounts of data, storing it in database systems. The data breach risk is compounded by the fact that cloud storage and processing are so common, putting even more sensitive information at risk from hackers and other security threats [2]. According to the literature, organizations need to engage in strong cybersecurity practices to protect data privacy and security. Additionally, the currently published research also shows there are no common cybersecurity protocols across all of Industry 4.0, and cyberattacks are evolving constantly [2]. Understanding these challenges is especially lacking in terms of frameworks for effective risk management and advanced approaches for detecting and monitoring cyberattacks.

Moreover, no studies are exploring the possibilities of technical disruption to society brought by the technologies of Industry 4.0, such as privacy leakage, social disturbance, social isolation, etc [3]. These research gaps highlight the requirement for more studies to ensure that the rewards are maximized while minimizing those risks to Industry 4.0.

To summarize, as revealed in the literature review, there are many significant cybersecurity challenges that industries adopting Industry 4.0 technologies can face, including, but not limited to, lack of standardized security protocols, system complexity, increased interconnectivity, and human-related vulnerabilities. These threats include advanced persistent threats (APTs), malware, distributed denial-of-service (DDoS) attacks, and insider threats [3]. Though some methods have been put into practice to ensure safety, including encryption, authentication, network segmentation, intrusion detection, and cybersecurity training, there are still major gaps and weaknesses. To combat emerging cybersecurity threats in Industry 4.0, researchers have proposed numerous mitigation strategies such as risk assessment, secure system design, continuous monitoring, and incident response planning. The other section of this review paper will analyze the key findings from the literature review and identify common themes and trends.

3. REVIEW METHODOLOGY

In the context of Industry 4.0 technology, this systematic review presents an in-depth analysis of the potential vulnerabilities affecting cyber security and mitigating strategies. A comprehensive systematic review was conducted to align with the present study. The review questions were devised to assess the advancement of cybersecurity in the context of Industry 4.0. The research questions (RQ) encompassed:

RQ1 - How has the field of cybersecurity in Industry 4.0 progressed in terms of the number of published papers about vulnerabilities, attacks, and defense strategies?

RQ2 - How has the progress been, in terms of the number of published papers, in the areas where vulnerabilities, attacks, and defense mechanisms intersect within the domain of Industry 4.0?

RQ3 - What are the cutting-edge mitigation strategies that address these challenges?

Firstly, keyword searches were conducted on relevant databases such as IEEE Xplore, Science Direct, and ACM Digital Library to identify relevant articles, journals, and conference proceedings. To conduct a thorough analysis, the study implemented a search strategy aimed at identifying all recent references about cyber-attacks, vulnerabilities, and mechanisms for prevention in Industry 4.0. The most significant phrases were particularly sought in the abstracts of the publications, while additional keywords were investigated in all metadata related to the studies. Each of the primary and secondary keywords used during the research are listed in Table. The above method ensured that all pertinent articles were discovered during the research process.

Table 1. Searched Keywords

Main Keywords	**Secondary Keywords**
Industry 4.0	Cyber Security
	Threats
	Vulnerabilities
	Risks
	Mitigation strategies
	Attacks defenses

Furthermore, a rigorous screening process was employed to eliminate any irrelevant articles that did not meet the study's criteria. This screening process consisted of a systematic evaluation of the titles, abstracts, and full texts of the articles. Articles meeting the specified inclusion criteria such as publication between 2010 and 2023 and being written in English, were exclusively chosen for further analysis. Similar trends and challenges regarding the cybersecurity of Industry 4.0 technologies were extracted from the selected articles. This low is realized by comparing the strengths and weaknesses of different approaches and determining the best approaches to minimize cybersecurity risks in Industry 4.0. The study methodology shown in Figure 2 was applied in such a way as to give a comprehensive insight regarding the threats of cybersecurity that Industrial 4.0 technologies are facing and how those threats can be mitigated effectively.

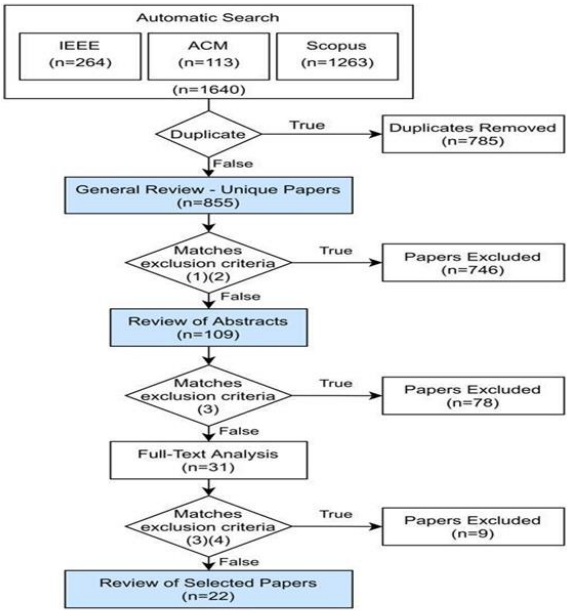
Automatic Search
IEEE (n=264)
ACM (n=113)
Scopus (n=1263)
(n=1640)
Duplicate
True
Duplicates Removed (n=785)
False
General Review - Unique Papers (n=855)
Matches exclusion criteria (1)(2)
True
Papers Excluded (n=746)
False
Review of Abstracts (n=109)
Matches exclusion criteria (3)
True
Papers Excluded (n=78)
False
Full-Text Analysis (n=31)
Matches exclusion criteria (3)(4)
True
Papers Excluded (n=9)
False
Review of Selected Papers (n=22)

Figure 2. Systematic Review Methodology

4. RESULT AND ANALYSIS

Data-driven technologies of Industry 4.0 have brought us into the new industrial revolution era [4]. These breakthroughs are transforming industries and revolutionizing production. At the same time, however, Industry 4.0 technologies have brought forth a new generation of cybersecurity threats that classical security solutions may not be able to cover appropriately [4]. The focus of this section lies in examining current literature on cybersecurity-related challenges and ways to overcome some of those challenges, especially through Industry 4.0 technologies.

Entities using Industry 4.0 technologies are susceptible to numerous cybersecurity risks and types of breaches. Data breaches, in which sensitive information is exposed or stolen, as well as system or network breaches, in which cybercriminals access a company's system or network without authorization, are the most common breaches. Figure 3 shows examples of other forms of breaches, e.g., denial-of-service (DoS) attacks, ransomware attacks, phishing attacks, etc.

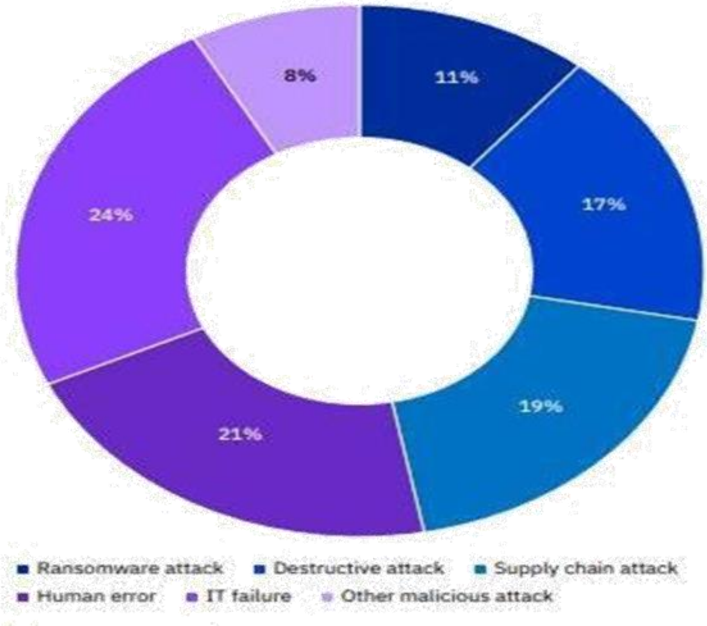

Figure 3. Types of breaches faced by Organizations [15].

Each of these types of cyberattacks has unique characteristics that require different prevention and mitigation strategies.

A. **Overview of Cybersecurity Challenges in Industry 4.0:-** Technologies Industry 4.0 technologies are not free from cyber problems; they have security challenges such as:

Absence of Standardized Security Standards – There are many sector-based communication protocols due to the availability of an array of Industry 4.0 technologies, and it is challenging to execute uniform security standards [5].

System Complexity – Many complex systems of hardware, software, and communication networks—all of which can be targeted by cyber threats.

Interconnectivity – Industry 4.0 technologies are much more interdependent than previous technologies, making them more vulnerable to cyberattacks.

Human Factor – Human factors such as human errors and social engineering attacks are major cybersecurity risks in Industry 4.0 environments [6].

IoT Safety – Internet of Things (IoT) devices play a critical part in Industry 4.0, but most of the IoT devices lack security [7].

Cost: Implementing robust cybersecurity measures can be expensive, particularly for small and medium-sized enterprises (SMEs) that may lack the financial aspect.

Resources to invest in cybersecurity.

Addressing these challenges requires a proactive cybersecurity approach that includes effective risk management, standardization of security protocols, and continuous monitoring investment in skilled cybersecurity talent.

B. Cybersecurity Threats in Industry 4.0 Technologies

Industry 4.0 technologies face various cybersecurity threats that can compromise their integrity, confidentiality, and availability [8]. These threats include:

Table 2. Numerous cyber threats that have an impact on Industry 4.0 technologies

Varying Cyber Threats Description	Varying Cyber Threats Description
Malware	It is typically distributed through infected emails, websites, or downloads, is software intended to damage, disrupt, or take control of computer systems
Phishing	A social engineering attack takes the form of phishing that deceives users into divulging sensitive information, usually through fraudulent emails or fake websites
Ransomware	The individual's contents encrypted are through using malicious program, and it subsequently demands ransom for deciphering the contents
DDoS Attacks	Attacks which involve entail inundating a system with traffic, thereby rendering it inaccessible to users
Insider Threats	Security threats may arise from employees or contractors who have access to sensitive information or systems.
Supply Chain Attacks	Supply chain attacks refer to exploitation of vulnerabilities in a company's supply chain, usually by targeting third part vendors and suppliers
IoT and OT Vulnerabilities	Security risks posed the use of IoT and devices, which can be difficult to secure and are often connected to critical system
Advanced Persistent	Sophisticated and Threats targeted attacks that involve a prolonged and ersistent effort to compromise a specific target.

1. **Advanced Persistent Threats (APTs):** These highly sophisticated and targeted cyber threats can evade detection for extended periods. APTs have the potential to infiltrate Industry 4.0 networks, steal sensitive data, and disrupt critical operations.
2. **Malware:** Malicious software, such as viruses, Trojans, and worms, can infect Industry 4.0 systems, leading to significant data loss and operational disruptions.
3. **DDoS Attacks**: Distributed Denial of Service (DDoS) attacks can slow down or completely disable Industry 4.0 operations, rendering systems inoperative.
4. **Insider Threats**: Both intentional and accidental actions by employees or contractors can cause severe harm to Industry 4.0 systems [9].
5. **Phishing Attacks:** Social engineering techniques, such as phishing, trick individuals into disclosing confidential information, often through fraudulent emails or fake websites.

Recent studies highlight the growing and significant threat of cyberattacks on organizations utilizing Industry 4.0 technologies. For instance, according to the Cyber Threat Defense Report published by Cyber Edge Group in 2021 [10], an alarming 85% of organizations experienced a successful cyberattack in the past year, as shown in Figure 4. This underscores the critical need for effective cybersecurity measures to safeguard Industry 4.0 systems and data from cyber threats.

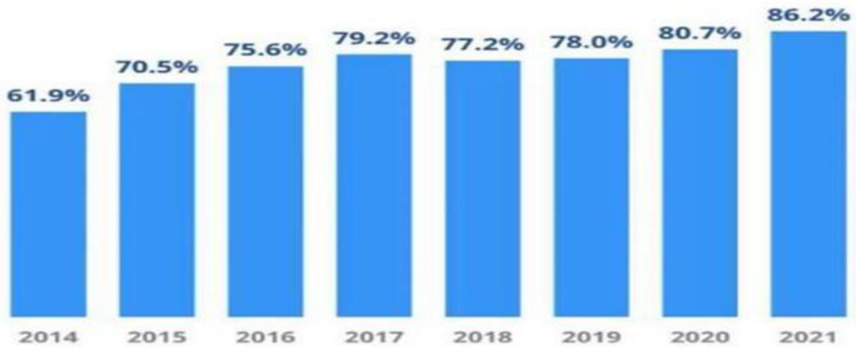

Figure 4. Organizations experienced at least one successful cyberattack [14]

Cybersecurity attacks can have a significant impact on Industry 4.0 technology, leading to production downtime, data loss, financial losses, and reputational damage. Therefore, companies must remain vigilant in identifying and mitigating cyber threats to protect their operations and safeguard their customers' sensitive information [11].

Cyber Security Measures in Industry 4.0 Technologies

Some cybersecurity practices have been adopted to mitigate the threats to cybersecurity that result from these technologies of Industry 4.0:

1. **Encryption and Authentication** – Tools for protecting Industry 4.0 systems from cyber threats based on encryption and authentication [12].

2. **Network Segmentation** – An effective way to divide network pathways into smaller segments to reduce the attack surface and prevent the spread of cyberattacks.

3. **Two-Factor Authentication (2FA)** – 2FA adds an additional layer of security to login credentials. Users have to go through two steps of authentication, such as entering a password and a one-time code sent to their smartphone or tablet. It enhances security and blocks unauthorized access [13].

4. **Vulnerability Scanning** – Continuous vulnerability scanning monitors networks and IT infrastructure for weaknesses that cybercriminals could exploit. This proactive approach enables businesses to address security risks before they become victims of an attack.

5. **Intrusion Detection and Prevention** – These systems are critical in protecting Industry 4.0 networks, as they actively identify and prevent cyberattacks from compromising the network [14].

6. **Cybersecurity Awareness Training** – Providing employees with education on cybersecurity best practices mitigates risks from human errors and social engineering attacks.

The article highlights that although these techniques greatly improve the security of Industry 4.0 technologies, companies need to constantly adapt to technological advancements to ensure adequate protection.

D. Mitigation Strategies for Risk Factors of Cybersecurity Challenges in Industry 4.0 Technologies

Various mitigation strategies have been suggested in response to security threats targeted at Industry 4.0 technology. Some of the most significant strategies include:

1. **Risk Analysis:** Conducting risk analysis helps identify, assess, and prioritize cybersecurity threats in Industry 4.0 technologies, enabling organizations to implement effective countermeasures [16].

2. **Secure-by-Design:** This principle ensures that Industry 4.0 technologies are designed with security in Each of these types of cyberattacks has unique characteristics that require different prevention and mitigation strategies. mind from the outset, rather than adding security measures as an afterthought.

3. **Access Controls:** Implementing access controls helps regulate who can access sensitive data and systems. This reduces the risk of unauthorized access and mitigates potential insider threats.

4. **Industry 4.0 Security Standardization:** Establishing uniform security protocols across Industry 4.0 technologies promotes a consistent approach to security across different devices and systems, minimizing vulnerabilities that cybercriminals might exploit.

5. **Continuous Monitoring:** Real-time monitoring allows organizations to detect and prevent cyber threats as they emerge, enabling a swift response to security incidents.

6. **Incident Response Planning:** Having a structured incident response plan in place enables organizations to mitigate the impact of cyberattacks on Industry 4.0 systems while ensuring business continuity [17].

7. **Data Interoperability:** Ensuring compatibility between data from various sources enhances analysis capabilities and allows for a faster response to emerging threats.

By implementing these countermeasures, organizations can strengthen their cybersecurity defenses in Industry 4.0. However, staying vigilant and keeping pace with evolving threats and technological advancements remains crucial for ongoing protection.

5. CASE STUDY

A. Honda Hit with WannaCry Ransomware Attack

In May 2017, Honda fell victim to the WannaCry ransomware attack, which compromised its production networks across multiple countries. This led to production stoppages and the temporary closure of some factories, highlighting the vulnerability of Industrial Control Systems (ICS) and Operational Technology (OT) systems to cyber threats. The attack also underscored the significant financial damage that such incidents can cause. Following the breach, Honda strengthened its cybersecurity strategy by implementing regular system maintenance and updates, network segmentation techniques, and rigorous employee training on cybersecurity best practices. Ransomware attacks are increasingly becoming a major cybersecurity threat for organizations utilizing Industry 4.0 technologies. According to a recent report, an alarming 63% of ransomware victims paid the ransom in the past year, further encouraging cybercriminal activity, as illustrated in Figure 5.

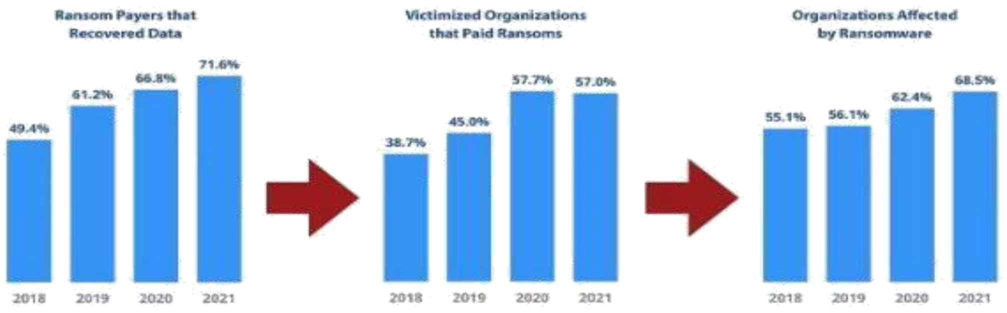

Figure 5. The ransomware vicious cycle [14].

But it also highlights the importance of taking proactive steps to combat ransomware and prevent the long-term financial and reputational damage it can cause.

B. Insider Threat at Tesla

In 2018, a disgruntled Tesla employee sabotaged the company's production system, causing delays and reducing output. This incident underscored the serious risks posed by insider threats to organizations using Industry 4.0 technologies. In response, Tesla enhanced access controls and security monitoring to mitigate the risk of similar incidents in the future.

C. Cloud Breach at Capital One

In 2019, Capital One suffered a cyber-attack targeting its cloud computing environment, exposing sensitive customer data. The attacker exploited a misconfigured firewall, revealing a vulnerability in the company's security defenses. This incident reinforced the need for strong access management, data loss prevention, and encryption in cloud-based systems. As a result, Capital One bolstered its cybersecurity framework by tightening access controls, encryption, and data protection measures.

D. Cyber Attack on the Ukrainian Power Grid

In 2015, a cyber-attack on the Ukrainian power grid led to a massive blackout, affecting thousands of people. The attackers gained access to the grid's Industrial Control Systems (ICS) and Operational Technology (OT) networks through a spear-phishing email. This incident underscored the vulnerability of critical infrastructure to cyber threats, similar to the 2021 Solar Winds attack, where hackers infiltrated U.S. government agencies and critical infrastructures to access sensitive data. In response, power grid operators implemented stronger access controls, advanced security monitoring tools, network segmentation, and regular system updates and patches.

E. Cyber Attack on the AIIMS Delhi

In November 2021, Chinese hackers targeted Indian seaports. Fast forward a year, and we witnessed another significant breach, this time at AIIMS—commonly referred to as the 'AIIMS hacking incident.' Of the 100 servers at AIIMS, 40 physical and 60 virtual, five of the physical servers were reportedly compromised by these hackers. On November 23rd, at 7 AM, several servers at AIIMS Delhi went down. Suspicion fell on Chinese or North Korean hackers. This attack forced the hospital to handle all services—outpatient, inpatient, and laboratory—manually. There were severe implications, such as the exposure of VIP personal data and patients' financial information, among many others. What's even more concerning is how long it took to clean up and restore the hacked servers.

As a nation celebrating its 76th year of independence, we need stronger laws to combat cybercrimes and better compliance for healthcare organizations. This incident should serve as a crucial learning point for national and state-level organizations to improve their compliance and build stronger cybersecurity defenses.

These case studies emphasize the necessity of effective cybersecurity measures in Industry 4.0 technologies to protect organizations from cyber threats.

6. RECOMMENDATION

1. **Standardized Security Frameworks:** Establishing standardized security frameworks for Industry 4.0 is vital in guiding the development and deployment of cybersecurity strategies. These frameworks help us discover and assess critical security risks to ensure they are mitigated.

2. **Increased Cooperation:** Cooperation between stakeholders is essential in addressing the complex and interlinked security threats presented by Industry 4.0. Through global collaborations between the private sector, academia, and governments, organizations can enable knowledge sharing, promote best practices, and enhance threat intelligence to increase the effectiveness of cybersecurity strategies

3. **Ongoing Monitoring and Evaluation:** Industry 4.0 technologies are dynamic, and hence cybersecurity threats and countermeasures need to be evaluated on a regular basis. This can be done through continuous risk assessments, gathering threat intelligence, and simulating incident response.

4. **Holistic Approach:** A well-rounded Industry 4.0 cybersecurity strategy must include technical, organizational, and human factors. These can encompass security controls like firewalls, encryption, organizational policies and procedures, and employee training and awareness programs.

5. **Supply Chain Security:** Modern supply chains are highly complex and interconnected, making supply chain security a significant challenge for Industry 4.0. Organizations should adopt a risk-based approach by assessing and monitoring supplier security, verifying the authenticity of components and products, and ensuring the secure transport of goods.

6. **Regulatory Compliance:** Compliance with cybersecurity regulations is critical in Industry 4.0, as many industries must adhere to laws governing data privacy, intellectual property protection, and overall security. Organizations should ensure they comply with all relevant laws and regulations through well-defined policies and procedures.

7. **Continual Improvement:** Cybersecurity is an ongoing process that requires continuous enhancement. Organizations must foster a culture of improvement by regularly evaluating their security posture, identifying vulnerabilities, managing threats, and ensuring proper remediation in case of security breaches. This approach helps

build resilience against emerging threats and allows organizations to adapt to evolving technologies and business needs [15].

7. CONCLUSION

In conclusion, Industry 4.0 technologies have revolutionized the way organizations operate and increased their efficiency and productivity. However, with these advancements, there are also increased cyber security challenges that organizations need to address. The use of interconnected and automated systems has made organizations more vulnerable to cyber-attacks, which can result in significant economic and reputational damages.

This review has identified some of the major cyber security challenges faced by organizations that use Industry 4.0 technologies. These include the lack of standardization, the use of legacy systems, the interconnectivity of systems, and the potential for insider threats. However, there are several strategies that organizations can implement to mitigate these risks. These include implementing a comprehensive cyber security program, including risk management strategies, access controls, network segmentation, and employee training on cyber security best practices.

In addition to these strategies, there are several recommendations that organizations can follow to strengthen their cyber security posture. These include regularly updating and patching systems, monitoring network traffic, implementing intrusion detection systems, and implementing strong access controls and encryption measures.

Furthermore, organizations should also collaborate with government agencies, regulatory bodies, and other stakeholders to develop and implement cyber security standards and guidelines that are specific to Industry 4.0 technologies.

Finally, it is important to note that cyber security is a continuous process, and organizations must remain vigilant in their approach to cyber security. They must regularly assess their cyber security risks and adapt their strategies to address new and emerging threats. By following these recommendations, organizations can better protect themselves against cyber threats and continue to leverage the benefits of Industry 4.0 technologies.

8. FUTURE RESEARCH AND SCOPE

While some challenges and mitigating measures are comprehensively covered in this research write-up related to cyber security in Industry 4.0 technologies, there continues to remain potential for greater investigation in this field of study. Future research could delve into the development of advanced technologies that are better equipped to address the evolving cyber security challenges of Industry 4.0, utilising block chain technology to enhance security and confidentiality of information, or taking advantage of artificial intelligence for threat detection systems. Furthermore, there is a need to investigate the implementation of cyber security standards and regulations in Industry 4.0 to bolster cyber resilience. Additionally, more studies are warranted to assess the impact of cyber-attacks on Industry 4.0 technologies, including their financial and reputational repercussions for businesses.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFRENCES

[1] G. Culot, F. Fattori, M. Podrecca and M. Sartor, Addressing Industry 4.0 Cybersecurity Challenges, IEEE Engineering Management Review, 2019.

[2] İ. İlhan and M. Karaköse, Requirement Analysis for Cybersecurity Solutions in Industry 4.0 Platforms, International Artificial Intelligence and Data Processing Symposium (IDAP), 2019.

[3] Ervural, B.C., Ervural, Overview of Cyber Security in the Industry 4.0 Era. in Industry 4.0: Managing The Digital Transformation. Springer Series in Advanced Manufacturing, 2020.

[4] Jamwal, A. Agrawal, R. Sharma, M. Giallanza, Industry 4.0 Technologies for Manufacturing Sustainability: A Systematic Review and Future Research Directions. Appl. Sci. 2021

[5] Bécue, A., Praça, I. & Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities 2021.

[6] Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts, Computers in Industry,2020.

[7] Lane Thames, Dirk Schaefer, Cybersecurity for Industry 4.0, 2018.

[8] N. Benias and A. P. Markopoulos, "A review on the readiness level and cyber-security challenges in Industry 4.0," 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA- CECNSM), Kastoria, Greece, 2017.

[9] A. Sivanathan and L. Zhu, "Cybersecurity challenges and opportunities in Industry 4.0," International Journal of Information Management,2020.

[10] Honda, “Honda Cyber Attack Fact Sheet,” Honda Newsroom, 2017.

[11] Tesla, “An Update on Last Week's Incident,” Tesla2018.

[12] Capital One, “A Message from our EO”,2019.

[13] U.S. Department of Homeland Security, Analysis Report on the Cyber Attack on the Ukrainian Power Grid”, 2016

[14] Cyber Edge Group, “Cyber Edge 2021 Cyber threat Defense Report” 2021

[15] Proaction International, Industry 4.0: Technologies to Kickstart Your Digital Transformation,2021

[16] Pankaj Pandey, Sokratis KatsikasThe future of cyber risk management: AI and DLT for automated cyber risk modelling, decision making, and risk transfer Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship, Edward Elgar Publishing, pp. 272-290 (2023)

[17] A. Bazzi, M. Chafii, Secure full duplex integrated sensing and communications. IEEE Trans. Inf. Forensics Secur., 19, pp. 2082-2097, 10.1109/TIFS.2023.3346696 (2024)