Volume 9, Issue 5, May – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

Cyber Security Systems in Manufacturing Process Application: A Review

Rakshith S.*[1]
Post Graduate Student of MTech on Machine Design at Department of Mechanical Engineering, RV College of Engineering, Bengaluru, Karnataka, India

Dileep L.[2]
Post Graduate Student of MTech on Product Design and Manufacturing at Department of Mechanical Engineering, RV College of Engineering, Bengaluru, Karnataka, India

Dr. Gopalakrishna[3]
H D is Professor and Associate Dean – PG Studies at Department of Mechanical Engineering, RV College of Engineering, Bengaluru, Karnataka, India

Corresponding Author: Rakshith S.*[1]

Abstract:- In recent times, technological progress has become increasingly pivotal across various sectors, particularly in engineering and its associated fields. However, organizations are grappling with numerous challenges, foremost among them being security threats such as unauthorized access to sensitive company data by external entities. The prevalence of such security issues has emerged as a significant concern for many enterprises, as the economic stability of an organization hinges on the secure integration of diverse information assets, free from external vulnerabilities. This study delves into existing literature on advancements in cybersecurity within manufacturing process networks, aiming to bolster safety measures against cyber-attacks and fortify operations. With the advent of Industry 4.0, there is a ripe opportunity to infuse modernizing elements into manufacturing systems, thereby fortifying their security infrastructure. By leveraging cybersecurity protocols, organizations can safeguard information integrity to uphold stringent safety standards effectively.

Keywords:- *Cyber Security, Industrial, Integrated Data, Manufacturing Systems, Smart Manufacturing.*

I. INTRODUCTION

The Digital manufacturing involves using computer-assisted applications to manage various manufacturing functions, with a forward-looking strategy poised for adoption across diverse industries. It heavily relies on Information and Communication Technology tools for support.

The primary objective of cybersecurity systems is to combat security threats within the shop floor environment, ensure confidentiality throughout every stage of the manufacturing operations cycle, restrict access to information solely to authorized individuals, and mitigate fraudulent activities during data processing. Despite encountering challenges, cybersecurity measures offer robust solutions to safeguard information securely. Recent technological advancements intersect with emerging domains such as Industry 4.0, Cloud computing, and Virtual Assist systems. Conventional manufacturing practices confront numerous challenges, necessitating the management of new risks within shop floor operations. The implementation of cybersecurity systems not only enhances data quality but also augments organizational productivity. Adequate financial investment is imperative for the effective deployment of cybersecurity controls within manufacturing environments. The maintenance of confidentiality and data integrity remains pivotal to ensuring seamless information flow devoid of unauthorized disclosures. The evolution of industry systems introduces cost-saving benefits in contemporary settings, urging transformation to accelerate manufacturing processes with enhanced precision while upholding data confidentiality through adherence to security standards. Cybersecurity systems strive for universal access to data and information within manufacturing environments. Employing appropriate communication protocols and network standards is critical for bolstering data reliability and operational quality without succumbing to external threats. Current manufacturing systems boast rapid responsiveness and highly efficient infrastructure for data processing and storage, incorporating password protection mechanisms to mitigate threats. Cybersecurity applications within manufacturing operations encompass regulating both inbound and outbound data flows while addressing fundamental risks. Hence, it is imperative for every company to establish security standards to fortify the manufacturing process seamlessly.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

➢ *Architecture of Cyber Security Applications in Manufacturing Station*

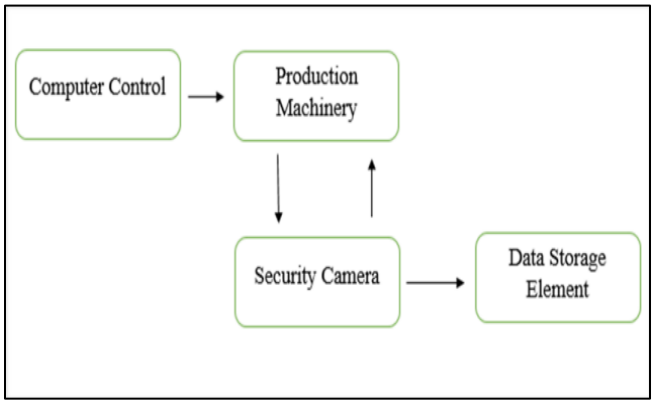

Fig 1: Architecture of Cyber Security Applications in Manufacturing Station

Figure 1 illustrates the operational procedure of cybersecurity systems within manufacturing settings. Initially, control is exerted by computer-assisted systems directly interfacing with production machine tools located on the shop floor. Periodically, security cameras monitor the acquired information to detect and deter unauthorized access or threats within the shop floor vicinity. Subsequently, the data captured by the security cameras is transmitted to the data storage component for archival and.

II. TYPES OF SECURITY SYSTEMS

A. Network Security

Network Security stands as the cornerstone of national productivity, underscoring the critical need for robust security measures to safeguard organizational operations. Thus, every manufacturing entity must institute adequate security protocols to mitigate various threats arising from information mishandling. The failure of network systems often precipitates these challenges. Network security encompasses protocols such as Data Loss Prevention and Identity Access Management.

B. Cloud Security

Cloud Security Amidst the current business landscape, organizations handle vast volumes of data on a daily basis, necessitating secure storage solutions like cloud services. Cloud security emerges as a paramount advantage in contemporary industry settings, offering heightened levels of security. Consequently, manufacturing organizations can leverage cloud storage to securely store their abundance of information for future access.

C. Application Security

Application Security Safeguarding both software and hardware from external threats requires the installation of antivirus programs on hardware devices. These programs serve to fortify the security of hardware assets against potential breaches.

D. Information Security

Information security prevents unwanted or unauthorized threats from accessing the information due to improper security infrastructure. The main aim of the information security system is to protect the information stored in hardware machinery, which is accessed and manipulated by software securely.

➢ *Challenges in Cybersecurity*

The primary challenge confronting manufacturing industries lies in effectively planning and implementing security measures tailored to the evolving nature of threats within their systems. Proactive measures are imperative to bolster security defenses against emerging threats.

➢ *Remedial Measures and Best Practices in Cybersecurity*

In the realm of cybersecurity, adopting remedial measures and best practices is crucial to fortify digital defenses against evolving threats. These measures encompass both technological frameworks and the actions of individuals who interact with digital systems.

A fundamental aspect of bolstering cybersecurity is exercising caution when sharing personal information online. It's essential to prioritize trusted websites and platforms when providing sensitive data, minimizing the risk of exposure to malicious actors.

Another key practice is to be vigilant about the security of URLs when entering sensitive information. Websites lacking secure protocols, indicated by "http://" rather than "https://", can pose significant risks. Avoiding such URLs helps mitigate the potential for data interception or manipulation.

Phishing attacks remain a prevalent threat in the digital landscape, often disguised as legitimate communications from reputable sources. Individuals should be wary of unsolicited emails, particularly those containing links or attachments from unknown senders. Refraining from interacting with such content reduces the risk of falling victim to phishing schemes.

Regularly updating devices and software is essential for addressing vulnerabilities that could be exploited by cyber threats. Outdated systems are particularly susceptible to attacks, as they may lack critical security patches and enhancements. By staying current with updates, individuals can mitigate potential security risks and strengthen their digital defenses.

Additionally, implementing robust data backup practices is vital for safeguarding critical information in the event of a cyber-attack. Regularly backing up files ensures that essential data remains accessible even in the face of data breaches or system compromises. This proactive measure can significantly mitigate the impact of cyber incidents on organizational operations and data integrity.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

Overall, maintaining vigilance and staying informed about online activities are central tenets of effective cybersecurity. By adopting these remedial measures and best practices, individuals can contribute to the protection of organizational assets and devices against cyber threats.

III. LITERATURE REVIEW OF CYBER SECURITY IN MANUFACTURING PROCESS OPERATIONS

This section provides an overview of existing literature concerning cyber security in manufacturing process systems.

- **Valentin Mullet et al. (2016)** have contributed insights into advancing Industry 4.0, the modern revolution integrating cutting-edge technologies such as IoT (Internet of Things) and Cloud Computing into manufacturing systems. Their focus on a limited number of articles highlights the objectives, methodologies, and solutions for cyber security implementation and standards within Industry 4.0.
- **Siva Chaitanya Chaduvula et al. (2018)** emphasize the significant improvements brought about by digital technologies, particularly in collaborative model network systems prevalent in today's manufacturing. They highlight the interconnectedness of manufacturing machines via sensors and computer support systems, underlining the importance of cyber security in safeguarding information through password protection against potential threats.
- **Nilufer Tuptuk and Stephen Hailes (2018)** discuss the global revolutionary changes underway in manufacturing systems, with increased investment in Smart Manufacturing Systems to address environmental shifts promptly. Their study delves into existing security systems, types of data loss attacks, safety awareness levels, and guidelines for safety monitoring and security alerts.
- **Uchenna P. Daniel Ani et al. (2017)** address the various challenges faced by manufacturing industries, including direct hacking of hardware and software resulting in compromised product quality and reputation. They advocate for the integration of resources—people, processes, and technology—to combat illegal cyber-attacks effectively.
- **Armando Araújo de Souza Junior et al. (2021)** explore the transformative impact of nextgeneration technology, particularly Industry 4.0, on manufacturing industries. They highlight the role of advanced cyber security systems in enhancing organizational infrastructure security to mitigate threats amidst rapid technological shifts.
- **Katariina Kannus Deloitte and Ilona Ilvonen (2018)** underscore the role of cyber security systems in enhancing data quality within manufacturing process automation. They emphasize securing information through various means to minimize threats, while also urging professionals to engage in research focusing on IoT, cloud computing, and other core areas shaping future manufacturing systems and operations. Their survey underscores IoT, Industry 4.0, and Smart automation as focal points in cyber security systems, urging professionals to innovate in addressing cyber security challenges within these domains.
- **Frank Cremer et al. (2022)** emphasized the prevalence of cybercrime cases, particularly within industrial systems, underscoring the significant financial investment, amounting to nearly 1 trillion USD globally, allocated towards addressing cybersecurity concerns. Their research amalgamated academic and industry-focused approaches to tackle diverse cybersecurity issues, prioritizing risk management and data access security.
- **Allesendro Fedelle and Cristian Roner (2022)** highlighted the escalating importance of cybersecurity across various sectors beyond manufacturing, such as banking and defense. Drawing on a collection of theoretical literature articles, they underscored the need for future research avenues within existing cybersecurity domains.
- **Bharadwaj R. K. Mantha and Borja García de Soto (2021)** noted the growing significance of cybersecurity in construction applications amid advancing digitalization. They advocated for domain-specific studies to address industry-specific challenges and constraints, particularly within construction, owing to the lack of awareness regarding cybersecurity practices in this domain.
- **Ricardo Jorge Raimundo and Albérico Travassos Rosário (2022)** stressed the integral role of security within IoT systems to safeguard data and infrastructure. Their review, based on 70 articles from prominent Scopus-indexed journals, highlighted ongoing debates and challenges in addressing cybersecurity issues within organizations.
- **Dharmesh Faquir et al. (2021)** highlighted the enhancement of communication protocols within industrial subsystems through smart grid technology, which surpasses traditional power grid systems in terms of productivity and security. They proposed modifications to computer network systems, including data encryption methods, to mitigate cybersecurity threats effectively.
- **Dazhong Wua et al. (2018)** discuss the objectives of digital manufacturing, aiming to produce highly customizable goods with improved quality and reduced costs by integrating Industrial Internet of Things (IIoT), big data analytics, cloud computing, and advanced robotics in production facilities. They highlight the transformative potential of sensing, computing, and wireless technologies, which enable a paradigm shift in manufacturing, while also acknowledging the significant threats posed by cyber-attacks to the manufacturing sector. Their paper offers a comprehensive review of cybersecurity in digital manufacturing systems, covering aspects such as system characterization, threat and vulnerability identification, control measures, and risk assessment, and it identifies challenges and future research directions.
- **Mohd Nasrulddin Abd Latif et al. (2021)** explore network protection measures for inventory security, emphasizing the management of digital security involving information technology systems, software, and supply chain networks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

They highlight the susceptibility of management systems to cyber threats such as digital terrorism, malware, and data theft, and advocate for common supply chain security practices to mitigate risks, including sole-sourcing from trusted vendors and isolating critical machinery from external networks.

- **Paul Theron (2018)** delves into smart manufacturing applications within industrial settings, recognizing its significance due to enhanced performance and flexibility. Through a comparative analysis between traditional manufacturing control and smart manufacturing with cyber network applications, Theron advocates for collaborative efforts between industry and education sectors to strengthen the connection and foster improvement in smart manufacturing technologies.
- **Jean-Paul A. Yaacoub et al. (2022)** explore the increasing integration of robotics across various industries and the associated security challenges. They highlight the potential risks posed by malicious attacks on robots, including unauthorized control manipulation, which could result in severe consequences such as loss of human lives and significant financial losses. Their study reviews security vulnerabilities, hazards, and primary security attacks within the robotics sector.
- **Alireza Zarreha et al. (2018)** address the growing attention towards cybersecurity challenges arising from the integration of production systems and the Industrial Internet of Things (IIoT). They analyze risk analysis factors, including the likelihood and impact of cyber attacks, and propose a game theory-based model to simulate the conflict between manufacturing systems and cyber attackers, considering cost functions to assess financial losses.
- **Alacer and Cruz Machado (2019)** discuss the digitization era catalyzed by Industry 4.0, wherein business models, production methods, equipment, personnel, goods, and services are digitized. They emphasize the real-time monitoring and control enabled by modern information and communication technology developments, transforming factories into intelligent entities that operate seamlessly across the entire value chain. Their analysis highlights the decentralized nature of applications in Industry 4.0, enabled by advanced digital technologies.
- **Jaco Prinsloo (2019)** highlights the growing prominence of three-dimensional (3D) printing in the manufacturing sector, particularly within the framework of Industry 4.0. He underscores the myriad benefits offered by 3D printing, including its superiority over traditional manufacturing methods in terms of efficiency, cost-effectiveness, and effectiveness. With the integration of 3D printing into the realm of the Internet of Things (IoT), manufacturing processes are transitioning into cyberspace, offering extensive opportunities for automation and optimization. However, despite its innovative potential, Prinsloo acknowledges significant concerns regarding cybersecurity threats associated with this transformative technology.
- **Rahayu Ahmad and Ramayah Thurasamy (2022)** conduct a systematic literature review to analyze studies related to cybercrime victimization using the Remote Access Trojans (RAT) theory. They categorize papers based on the types of cybercrimes investigated, including those dependent on cybercrime (such as hacking and malware) and those enabled by cybercrime (such as phishing, fraud, and identity theft). Their findings suggest the need for a more precise application and interpretation of the RAT theory to address measurement inconsistencies and ambiguities in cybercrime victimization. They advocate for longitudinal research to discern the impact of the RAT construct before and after cybercrime incidents.
- **Abhijeet Ghadge et al. (2022)** observe a scarcity of inter-firm-based cyber risk studies despite heightened research interest in cybersecurity. To address this gap, they explore cyber risk management within supply chain contexts through a systematic literature evaluation. Their approach involves selecting papers from various transdisciplinary fields published between 1990 and 2017 and conducting descriptive and thematic analyses using data mining techniques to facilitate a comprehensive, repeatable, and transparent assessment of cyber risk typologies and management strategies within supply chains.

➢ *Cyber Security Challenges Affecting the Manufacturing Industry*

Securing manufacturing applications presents unique cybersecurity challenges due to the convergence of operational technology (OT) and information technology (IT). Legacy industrial systems often lack built-in security features, making them vulnerable to attacks. The interconnectedness of devices within smart factories increases the attack surface, amplifying risks of data breaches, sabotage, and production disruptions. Protecting intellectual property and sensitive data amidst complex supply chain networks is paramount. Additionally, ensuring the safety of IoT devices and maintaining regulatory compliance further complicate cybersecurity efforts. Addressing these challenges requires a holistic approach integrating robust defenses, regular updates, employee training, and proactive risk management strategies.

➢ *Potential Risks Posed by Manufacturing Systems*

A study conducted by cyber insurance firm Allianz reveals that industrial control systems (ICS) are increasingly targeted in cyber-attacks against critical infrastructure, with a focus on disrupting operations rather than data theft. Notably, 54% of critical infrastructure suppliers reported attempts to manipulate systems, while 40% reported attempts to shut down systems. Manufacturers face heightened susceptibility to attacks aimed at disrupting operations for prolonged periods. Moreover, they are highly sensitive to the theft of proprietary trade secrets and consumer data. This underscores the critical need for all manufacturers, particularly those within the Defense Industrial Base (DIB) industry, to remain vigilant and prioritize robust cybersecurity measures.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

➢ *Example of Disruptive Cyber-Attack at Honda Plant*

The surge in cyber-attacks observed in 2020 can likely be attributed to the organizational adjustments made in response to the COVID-19 pandemic. Particularly concerning are phishing scams, which serve as a potential entry point for ransomware operations, posing significant risks to remote employees. Ransomware typically encrypts data until a ransom is paid, effectively paralyzing entire production lines, as revealed by research from cyber insurer Beazley in June 2020, which documented the highest growth in ransomware attacks during the first quarter of 2020 across industries. Manufacturers have been disproportionately impacted by these malicious activities.

For manufacturers, managing increasingly dispersed and diverse infrastructure networks presents significant challenges. Embracing Industry 4.0 technologies further complicates the task of establishing and maintaining accurate real-time inventories of OT/IoT systems and devices. However, it is imperative for manufacturers to possess the capability to monitor network conditions in real-time and understand device behavior to formulate effective cybersecurity policies for both OT and IT systems. Timely detection of anomalous activities is crucial to prevent operational disruptions caused by maintenance issues or cyber-attacks. A notable challenge lies in the inadequacy of basic threat intelligence data concerning assaults targeting OT and IoT infrastructure. Cybersecurity teams must be equipped to detect, analyze, and respond to indicators of compromise (IOCs) and abnormal network behaviors.

The widespread deployment of IoT devices provides hackers with numerous entry points into networks, enabling lateral movement. Consequently, implementing network segmentation is integral to OT cybersecurity solutions. According to the 2019 Deloitte and MAPI Smart Factory Study, 40% of surveyed factories experienced a cyber-event over a 12-month period, impacting their operations significantly of those affected, 87% reported instances of unauthorized infrastructure access, 86% encountered operational disruptions, and 85% experienced theft of intellectual property, as illustrated in Fig. 2.

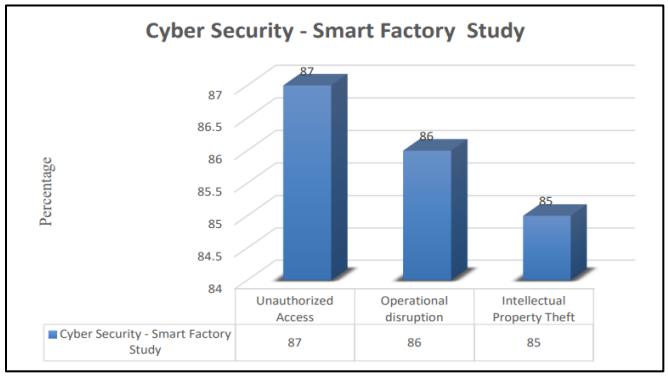

Fig 2: Statistical Findings from the 2019 Deloitte and MAPI Smart Factory Study

IV. RISK REDUCTION STRATEGIES IN CYBERSECURITY APPLICATIONS

➢ *Effective Risk Reduction Strategies in Cybersecurity Applications Include:*

Reducing risks in cybersecurity applications involves several key strategies. First and foremost, it's essential to utilize the tools and methods provided by the vendor to locate operational technology (OT) assets. These tools are specifically designed to identify and manage assets within your network, helping to ensure comprehensive coverage and visibility.

Leveraging openly accessible mapping tools for passive networks can provide valuable insights into the overall network infrastructure. By understanding the layout and interconnectedness of systems, organizations can better assess potential vulnerabilities and plan accordingly.

A crucial step in risk reduction is confirming the accuracy of the OT infrastructure map through physical walkthroughs. This hands-on approach allows for the validation of existing documentation and helps identify any discrepancies or overlooked components.

Keeping software and firmware up to date with the latest versions is another fundamental aspect of cybersecurity risk mitigation. Regular updates often include patches and security enhancements that address known vulnerabilities, reducing the likelihood of exploitation by malicious actors.

It's important to include process logic and OT programs in vulnerability management efforts. This ensures that all aspects of the operational environment are considered when implementing mitigations and security controls.

When addressing known vulnerabilities, organizations should prioritize the use of mitigations such as patches and offsetting security controls. These measures help to minimize the risk of exploitation while longer-term solutions are developed and implemented.

Incorporating vendor-provided programming and diagnostic tools into cybersecurity practices can also enhance risk reduction efforts. These tools are specifically tailored to the equipment and systems in use, allowing for more efficient monitoring and maintenance.

Monitoring and reviewing authorized external access connections for misuse or unusual activity is essential for detecting and responding to potential security incidents. By maintaining detailed logs and regularly reviewing access logs, organizations can quickly identify and mitigate threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

In situations where remote access to process controllers is necessary, disabling remote program mode while controllers are in use can help prevent unauthorized access and manipulation of critical systems.

Finally, implementing controls to lock or limit set points in control processes can help prevent unauthorized changes that could lead to disruptions or compromises in system integrity. By restricting access to critical settings, organizations can reduce the risk of malicious interference and maintain operational stability.

- *Cryptography*

For Securing Data in Transit Cryptography, encompassing encryption and decryption phases, safeguards data during transmission through communication channels. By employing suitable encryption algorithms before transmitting data, and corresponding decryption algorithms at the receiving end, potential hackers are deterred from intercepting and compromising sensitive information. Various encryption algorithms, as discussed in Panneerselvam (2016), offer robust security measures.

V. CONCLUSION

This paper undertook an extensive literature review to explore prevalent issues in cybersecurity within manufacturing applications. Notably, confidentiality and safety are increasingly vital in industrial settings, given the rising occurrences of cyber-related thefts and fraud globally. The findings underscore the prevalence of unauthorized data access by third parties, necessitating stringent security measures across manufacturing processes. Moreover, adherence to standardized procedural guidelines for security-related threats is imperative across all industries, underscoring the importance of implementing robust security protocols. Thus, this paper aimed to provide a comprehensive overview of cybersecurity dimensions across diverse applications.

REFERENCES

[1]. V Mullet, P Sondi and E Ramat (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0, IEEE Access, 9, 23235-23263, Available at: https://doi.org/10.1109/ACCESS.2021.3056 650.

[2]. S Chaitanya Chaduvula, A Dachowicz, M J. Atallah and J H. Panchal (2018). Security in cyber-enabled design and manufacturing: A survey, Journal of Computing and Information Science in Engineering, 18(4), Available at: https://doi.org/10.1115/1.4040341.

[3]. N Tuptuk and S Hailes (2018). Security of smart manufacturing systems, Journal of Manufacturing Systems, 47, 93-106, Available at: https://doi.org/10.1016/j.jmsy.2018.04.007.

[4]. U P. Daniel Ani, H (Mary) He and A Tiwari (2016). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, Journal of Cyber Security Technology, 1(1), 32-74, Available at: https://doi.org/10.1080/23742917.2016.125 2211.

[5]. A Araújo de Souza, J Luiz de Souza Pio, J Cunha Fonseca, et al (2021). The state of cybersecurity in smart manufacturing systems: A systematic review, European Journal of Business and Management Research, 6(6), 188-194, Available at: https://doi.org/10.24018/ejbmr.2021.6.6.11 73.

[6]. K Kannus Deloitte and I Ilvonen (2018). Future prospects of cyber security in Manufacturing: Findings from Delphi study. Proceedings of 51st Hawaii International Conference on systems sciences. Scholar Space, Available at: https://scholarspace.manoa.hawaii.edu/item s/b640e9b8-c8f3-43cc-aa41-ae2e43803edf.

[7]. F Cremer, B Sheehan, M Fortmann, et al (2022). Cyber risk and cybersecurity: a systematic review of data availability, Geneva Papers on Risk and Insurance: Issues and Practice, 47(3), 698-736, Available at: https://doi.org/10.1057/s41288-022-00266- 6.

[8]. A Fedelle and C Roner (2022). Dangerous games: A literature review on cybersecurity investments, Journal of Economic Surveys, 36(1), 157-187, Available at: https://doi.org/10.1111/joes.12456.

[9]. R. K. Mantha Bharadwaj and B García de Soto (2021). Cybersecurity in construction: Where do we stand and how do we get better prepared, Frontiers in Built Environment, 7, Available at: https://doi.org/10.3389/fbuil.2021.612668.

[10]. R Jorge Raimundo and A Travassos Rosário (2022). Cybersecurity in the internet of things in industrial management, Applied Sciences, 12(3), Available at: https://doi.org/10.3390/app12031598.

[11]. D Faquir, N Chouliaras, V Sofia, et al (2020). Cybersecurity in smart grids, challenges and solutions, AIMS Electronics and Electrical Engineering, 5(1), 24-37, Available at: https://www.aimspress.com/aimspressdata/electreng/20 21/1/PDF/ElectronEng-05- 01-002.pdf.

[12]. D Wu, A Ren, W Zhang, et al (2018). Cybersecurity for digital manufacturing, Journal of Manufacturing Systems, 48(C), 3-12, Available at: https://doi.org/10.1016/j.jmsy.2018.03.006.

[13]. L Mohd Nasrulddin Abd, A Nurul Ashykin Abd, H Nik Syuhailah Nik and A Zuraimi Abdul (2021). Cyber security in supply chain management: A systematic review, LogForum, 17(1), 49-57, Available at: http://dx.doi.org/10.17270/J.LOG.2021.555 .

[14]. P Theron (2018). Through-life cyber resilience in future smart manufacturing environments. A research programme, Procedia Manufacturing, 16, 193-207, Available at: https://doi.org/10.1016/j.promfg.2018.10.15 7.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1800

[15]. J-Paul A. Yaacoub, H N. Noura, O Salman and A Chehab (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations, International Journal of Information Security, 21, 115-158, Available at: https://doi.org/10.1007/s10207-021-00545- 8.

[16]. A Zarreha, C Saygin, H Da Wan, et al (2018). Cybersecurity analysis of smart manufacturing system using game theory approach and quantal response equilibrium, Procedia Manufacturing, 17, 1001-1008, Available at: https://doi.org/10.1016/j.promfg.2018.10.08 7.

[17]. V. Alcácer and V. Cruz-Machado (2019). Scanning the industry 4.0: A literature review on technologies for manufacturing systems, Engineering Science and Technology, an International Journal, 22(3), 899-919, Available at: https://doi.org/10.1016/j.jestch.2019.01.006 .

[18]. J Prinsloo, S Sinha and B von Solms (2019). A review of industry 4.0 manufacturing process security risks, Applied Sciences, 9(23), Available at: https://doi.org/10.3390/app9235105.

[19]. R Ahamed and R Thurasamy (2022). A systematic literature review of routine activity theory's applicability in cybercrimes, Journal of Cyber Security and Mobility, 11(3), 405-431, Available at: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/12451/13563.

[20]. A Ghadge, M Weiß, N D. Caldwell and R Wilding (2020). Managing cyber risk in supply chains: a review and research agenda, Supply Chain Management, 25(2), 223-240, Available at: https://doi.org/10.1108/SCM-10-2018- 0357.

[21]. Anand E, Panneerselvam R. (2016). A study of crossover operators for genetic algorithm and proposal of a new crossover operator to solve open shop scheduling problem, American Journal of Industrial and Business Management, 6(6),774-789, Available at: https://www.scirp.org/journal/paperinformation.aspx?paperid=67660