Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20240302030
Volume 3, Issue2 (May-August 2024), PP: 192-201.
www.indjcst.com
ISSN No: 2583-5300

Enhancing Cybersecurity in Smart Manufacturing: A Comprehensive Approach

Anupriya Bharti[1], Dr. Bramah Hazela[2]
[1] *PG student, Department of Engineering and Technology, Amity University, Lucknow, Uttar Pradesh, India.*
[2]*Assistant Professor G-III and Program Leader, Amity University, Lucknow Campus, Lucknow, Uttar Pradesh, India.*

To Cite this Article: *Anupriya Bharti[1], Dr. Bramah Hazela[2], "Enhancing Cybersecurity in Smart Manufacturing: A Comprehensive Approach", Indian Journal of Computer Science and Technology, Volume 03, Issue 02 (May-August 2024), PP: 192-201.*

Abstract: *The industry 4.0 defines a new era of much efficient and intelligent manufacturing processes that works in integration with other advanced technologies like AI, Big data, Block chain, etc. The smart manufacturing industry has remarkably evolved due to integration of advanced technologies like cyber-physical systems (CPS), Internet of Things (IoT), digital twins that makes up a highly connected infrastructure where data flows in real time. However, the involvement of these technologies has also significantly increased the exposure of manufacturing industry to the cyber threats.*

This article investigates several security challenges and major threats that are associated with the manufacturing industry. It evaluates various security implementations including digital twins, machine learning, and block chain based on their effectiveness, scalability, and feasibility in terms of security. Through a comprehensive literature review, case study analysis of notable cyberattacks and qualitative exploratory methods, this study explores the best line of defence against the cyber threats.

Our findings highlight the critical role of robust and adaptive multiple line of defense mechanisms in mitigating cyber risks. The research concludes by emphasizing the need for an effective security strategy that combines advanced technological solutions with continuous employee education and proactive threat management to safeguard smart manufacturing processes against evolving cyber threats.

Keywords: *Smart manufacturing, Cybersecurity, Digital Twin, Industry 4.0, Cyberattack, PERA model.*

I.LITERATURE REVIEW

In the course of time, the digital twin technology has experienced a remarkable change driven by advanced technologies like AI, CPS and IoT. In around 1970 when NASA encountered a series of problems that included damaged oxygen tanks during the launch of Apollo 13, they used a prototype to test different solutions to eliminate the problem. This was the first time; simulation was used to experiment on virtual prototype of Apollo 13 and determine the best course of action for the situation. In 2002, John Vickers a principal Technologist at NASA, first originated with the term "digital twin" which was later explained in [1] as – "an integrated Multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin". In following years, the digital twin technology flourished remarkably attaining a special purpose in the field of manufacturing [1-4], healthcare [5,6], aerospace [7] and many more. The definition of digital twin technology is differently perceived by the authors based on its applications and its abilities.

Table 1. Definitions of digital twins

Author	Definitions
NASA 2012 [1]	"A Digital Twin is an integrated Multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin."
Y. Chen 2017 [8]	"A digital twin is a computerized model of a physical device or system that represents all functional features and links with the working elements"
Z. Liu, N. Meyendorf, and N. Mrad 2018 [9]	"The digital twin is actually a living model of the physical asset or system, which continually adapts to operational changes based on the collected online data and information, and can forecast the future of the corresponding physical counterpart"

Y. Zheng, S. Yang, and H. Cheng 2018 [10]	"A Digital Twin is a set of virtual information that fully describes a potential or actual physical production from the micro atomic level to the macro geometrical level"
R. Vrabîc, J. A. Erkoyuncu, P. Butala, and R. Roy 2018 [11]	"A digital twin is a digital representation of a physical item or assembly using integrated simulations and service data. The digital representation holds information from multiple sources across the product life cycle. This information is continuously updated and is visualised in a variety of ways to predict current and future conditions, in both design and operational environments, to enhance decision making"
A.Madni, C. Madni, and S. Lucero 2019 [12]	"A Digital Twin is a virtual instance of a physical system (twin) that is continually updated with the latter's performance, maintenance, and health status data throughout the physical system's life cycle"
Tao, Fei, Meng Zhang, and Andrew Yeh Chris Nee 2019 [13]	"Digital twin is a virtual representation of a physical object or system that interacts with each other throughout the processes in its lifecycle."
T. Bergs, S. Gierlings, T. Auerbach, A. Klink, D. Schraknepper, T. Augspurger 2021 [14]	"A digital twin is an automatic two-way connection between real-world and virtual simulation in digital twin spaces"

Throughout the years, the digital twin technology has dramatically evolved in terms of simulation, connectivity, intelligence, and visualization. The number research articles containing keywords "digital twins" and "smart manufacturing" showed an exponential growth after concept the of Industry 4.0 in 2014 (Google Scholar numbers) which focused on cyber-physical systems. The introduction of CPS systems has been a significant instrument in shaping Industry 4.0 and digital twins.

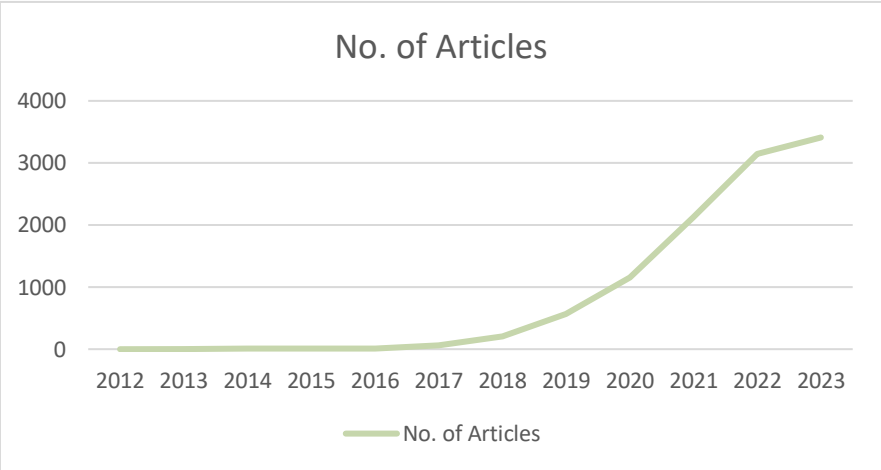

Figure 1. Article count according to Google scholar

The timeline of digital twins started from early 1970s with the launch of Apollo 13 when we only had technologies for computational modelling. In 1990s, with the concept of CAD (Computer-Aided Design) we were able to digitally represent a physical object. In 2002, the term "digital twin" was first used by University of Michigan during a presentation. [1]

In 2006, the term "smart process manufacturing" was coined at National Science Foundation workshop on Cyberinfrastructure. It was later shortened as "smart manufacturing" which focused on highly connected environment of information-driven manufacturing equipment. [15] On the other hand, in 2014, Germany released a Roadmap version of "Industry 4.0" was published.

The concept of industry 4.0 focused more on integration of data-enabled "smart products" with cyber-physical systems. [16] Along with evolving simulation techniques, other enabling technologies including IoT, Cloud computing were also introduced. These technologies were later integrated with the digital twin technologies which drastically changed the industry of manufacturing.

In 2016, MESA International published a report titled "smart manufacturing landscape explained" which discussed opportunities and challenges for the manufacturers. [17] A month later in the same year NIST published "Current standards landscape for smart manufacturing systems" that defined standards for manufacturing environments. [18]

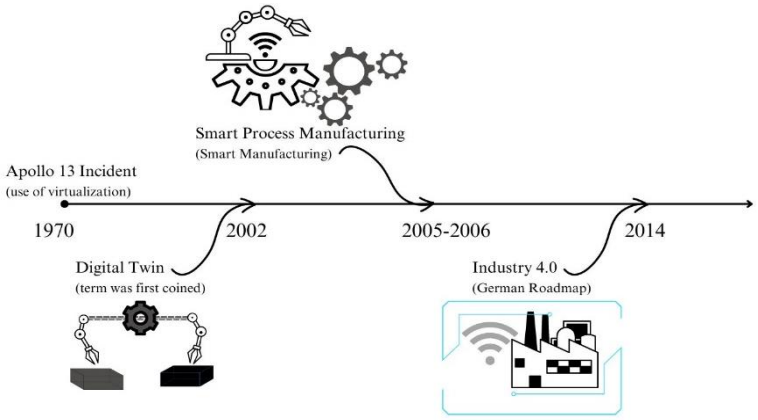

Figure 2. Timeline of Smart Manufacturing

With increase in connectivity and accessibility, the security risks and concerns also emerged. The cyber-attacks target different components of the smart manufacturing environment like IoTs, HMIs, Digital twins, IPCs, PLCs, etc. This article presents the structure of manufacturing industry, threats and risks associated with it, impact of attacks on the industry, standards, security practices, and advanced technologies for securing the smart manufacturing environment. This article aims to provide a summarize current threat scenario, possible risks and solutions associated with smart manufacturing environment.

I.INTRODUCTION

The manufacturing industry has greatly evolved in the past few years. The involvement of IT technologies has not only built the foundation of Industry 4.0, but also has increased the exposure of the manufacturing sectors to the cyberattacks. The smart manufacturing environment is a highly connected architecture that involves real-time, data-driven processing of data. The connectivity and data transfer allows real-time monitoring, predictions, process optimization and improve overall operational efficiency. The ability to collect, analyse, and act on data in real-time is what makes smart manufacturing truly intelligent and efficient, highlighting the critical importance of data in this modern industrial paradigm.

The main principle of smart manufacturing revolves around scalability, security, inoperability, and energy efficiency. With time various techniques have emerged that make such an infrastructure possible. On the other hand, cyber attackers have also evolved and come up with new techniques to invade the security of manufacturing environment every day. The attackers try to infect the infrastructure with the malicious code to gain control over components. Detecting attacks or malicious code in every system is quite challenging. Therefore, it is important to establish and implement security practices in an organization to identify and mitigate risks.

This article highlights the major vulnerabilities of smart manufacturing industry that can be a target of cyberattack. It also describes how advanced technologies can help to contribute to security of the manufacturing environment. Later on, it also discusses the major standards, compliances, and basic security practices that are needed to be practiced and followed by an organization.

The article starts with a brief introduction of smart manufacturing infrastructure followed by major threats and risks involved with it. Then it proceeds with the standards and compliances, important security practices that should be implemented in any organization. Later on, it describes the advanced technologies and their comparison based on their feasibility, scalability, and effectiveness in contributing to the security of manufacturing industry. Lastly, some of the major case studies that involved notable cyberattacks in manufacturing industry have been discussed along with the lesson learned from each of them.

II.SMART MANUFACTURING INFRASTRUCTURE

The smart manufacturing components and infrastructure varies from industry to industry. To understand the basic industrial architecture, we will consider the general structure of Operational Technology (OT). The OTs are a collection of hardware and software designed for controlling and monitoring the industrial processes. The OTs include various technologies and protocols divided into different levels.

Operational Technologies further contain ICS (Industrial Control Systems) which includes dedicated network and tools for monitoring and controlling industrial operations like SCADA (Supervisory Control and Data Acquisition), RTU (Remote Terminal Units), PLC (Programmable Logic Units), DCS (Distributed Control Systems) and many more.

These technologies together allow better control and vision over the industrial process. OT technologies generally contain the machinery and industrial processes which are combined with IT technologies to enable smart manufacturing and Industry 4.0. The IT technologies include IoT devices, cloud computing, Digital twin technology, Big Data, Networking, Database Management, and many more which allows better management, analysis, simulation, and effective handling of large amount of data. Merging OT and IT technologies enables the concept of smart manufacturing. The benefits include enhanced decision making, automation, optimization for low cost, mitigating risks, improved scalability, and business profits.

The IoT devices used for industrial processes like manufacturing, supply chain management, monitoring, etc are known as IIoT. The IIoT devices are a result of merging the OT and IT technologies. The emerging threats in industrial environment are becoming more and more challenging day-by-day which is a result of dynamically evolving of OT and IT technologies. [19]

2.1 PERA model

The Purdue model or Purdue Enterprise Reference Architecture (PERA) is a reference model used to understand the enterprise architecture. The smart manufacturing industry includes both OT and IT technologies collaborated with each other to form a smart environment. [20]

The three zones: Enterprise Zone, Demilitarized Zone, Manufacturing Zone

It mainly consists of levels 0 to 4 based on the technologies and processes running in the industrial environment. The brief description of each level is as follows:

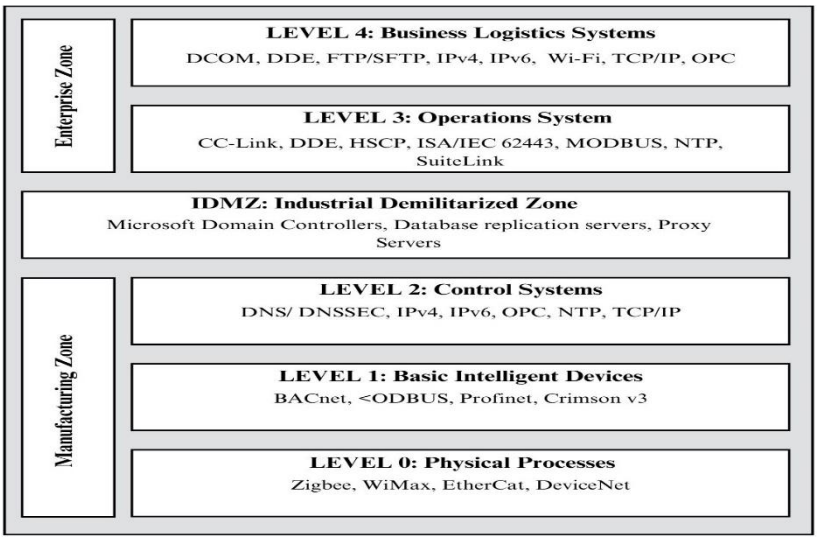

Figure 3. PERA model and its protocols

Level 0: Physical Processes

The level 0 consists of actual physical processes and equipment used to control and monitor the manufacturing processes. Level 0 systems include cyber-physical systems, sensors, actuators, and many other devices used to carry out the manufacturing.

Level 1: Basic Intelligent Devices

This level contains intelligent devices including analysers, IEDs (Intelligent Electronic Devices), PLCs (Programmable Logic Computers), etc. that are designed to behave in a certain way when specific conditions are met.

Level 2: Control Systems

Control system level includes monitoring and controlling systems and technologies like SCADA, HMI, and real-time control.

Level 3: Operation Systems

This level includes management of operational level processes that includes production and quality checks, management of middleware and execution systems.

Industrial Demilitarized Zone

The demilitarized zone is a barrier between enterprise zone and manufacturing zone serving as a perimeter that enables secure network connections between the two zones. It helps to keep divide the outer network that includes connection to the internet and inner network that includes communication between devices in the manufacturing ecosystem. The paper [21] describes the importance of IDZ and how it enhances cyber security of the overall environment. It also investigates the performance of the IDZ based in multiple factors such as response time, throughput, and FTP server load.

Level 4: Business Logistics Systems

The business logistics systems involve management of different business processes. Internet connectivity, IT processes that support production systems are found on this level. At this level, the logistic processes like managing schedules are carried out. The application servers, file servers, database servers, supervising systems also lie on this level.

III.CYBER RISKS AND THREATS IN SMART MANUFACTURING INDUSTRY

The smart manufacturing environment consists of several small and critical components that has monitoring, maintenance, and security requirements. These components can be classified into three categories: The physical assets, The Networks, The Critical Infrastructure

The physical assets such as sensors, actuators, cyber-physical systems, network devices, servers, etc. require physical security and maintenance. These assets are a crucial part of industry that build up the manufacturing environment on physical level.

The networks in industry are essential part of smart manufacturing that enables communication and collaboration among the smart devices. The internal network comprises of the link among the devices and monitoring systems in a traditional manufacturing environment whereas the outer network includes connecting industries from different locations to internet and cloud and enabling businesses to use big data analysis and remote monitoring of all the industrial sites. The outer network was introduced in smart manufacturing Industry 4.0. The network perimeter in manufacturing infrastructure can be defined as an outermost boundary between internal network and the cloud. This serves as a security perimeter including firewalls, IDS and IPS systems.

The critical infrastructure is basically a collection of any physical or logical assets that are sensitive. Any harm to these could cause a havoc in a business. These can include the program flow code, Human-Machine Interface (HMI), cyber-physical systems, etc. The critical infrastructure in an industrial environment are foundation of any manufacturing business and any loophole in security of this infrastructure can impact safety, economy and data breaches causing loss in trust and business reputation in market.

The smart manufacturing environment presents its own set of challenges that makes this infrastructure vulnerable. Many types of cyberattacks such as malware, phishing, spyware, sniffing, etc. can affect the processes and services running in the environment. Firstly, the vast network and multiple devices connected to the network create network complexities. Unorganized infrastructure and lack of management leads to compromised systems and poor incident response plans making it difficult to detect unusual activities or potential threats. Secondly, evolving with new security trends and threats requires professional training to make sure the infrastructure is properly secured. The security professionals ensure that all the systems are up-to-date, and they also implement new techniques and security controls for defence against network threats. Lack of security professionals to cut costs is a very common vulnerability seen in most of the organizations. This leads to lack of preparedness and weak risk management.

3.1 Vulnerabilities in OT and OT Threats

The smart manufacturing is directly connected to the internet which makes it highly collaborative and accessible. This connectivity is also allowing attackers to discover and exploit vulnerabilities such as weak passwords and unsecure remote access can cause unauthorized access and compromise the entire system. The mismanagement of permissions in network, poorly segmented or unsegmented networks, unconfigured firewalls, outdated protocols are some of the most common vulnerabilities that might incur in a smart manufacturing industry.

Some of the threats associated with manufacturing systems are as follows:

Unauthorized Access

The manufacturing industry consists of several manufacturing processing units connected with networks and internet. The exposed systems are prone to attacks allowing attackers to exploit vulnerabilities of the system to gain unauthorized access or control over industrial processes and files.

The attackers gather basic information like open ports, encryption techniques, operating system used in the systems that is used in later stages in implementing attack. The zero-day attacks are very common that are used by attackers to exploit weakly maintained or outdated protocols. Outdated protocols and systems are in fact a great threat to entire manufacturing system with large number of exploitable vulnerabilities.

HMI- based Attacks

Human-Machine Interface (HMI) is the core hub that enables interaction between users and machine to control and monitor the machinery via a software program. The interface helps to directly access the manufacturing processes and make it easier to understand and analyse the workflow. There are no specific global standards that are implemented to secure these systems leading to security breaches. These are a sensitive part of a smart manufacturing industry and an attack or control over these interfaces can lead to several damages and loss to the manufacturing business.

HMI-based attacks techniques such as memory corruption, buffer overflow, code injection, etc can lead an attacker to gain full control over all the files, workflow, and even physical assets. It can lead the attacker to physically damage the SCADA systems, collect operational data and even control over cyber-physical systems by interacting with digital twins.

Malwares

Malwares are most installed from an outer source or internally by an insider threat entity. Attackers detect vulnerabilities to exploit the older or outdated systems to install malwares and perform various attacks. In some cases, if the attacker knows the operating systems running on the victim machine they can build machine-specific malwares to target SCADA and ICS.

Email phishing is another very common attack that tricks the victim into thinking that it is legitimate and encourages them to download the files and payloads that help them to inject malwares in the system and exploit the system internally.

Some very common industry related malwares are PIPEDREAM and INDUSTROYER. PIPEDREAM is an attack framework containing a set of tools to scan and gain control over SCADA systems. INDUSTROYER was discovered in 2016 when it was used to disrupt the power supply in in Ukraine. In 2022, it was witnessed again with some additional features to target industry-based power grids which was named INDUSTROYER V2.

Side Channel Attack

Side-channel attack was first observed in 2007 according to **CVE-2007-3108** observed local users conducting a side-channel attack and retrieve RSA private keys [22]. This attack basically observes the physical implementation using various techniques such as time analysis and power analysis. By observing the physical changes and implementation, the attacker can figure out the messages, passwords and in worse cases the encryption techniques.

In time analysis, the attacker runs a loop to enter password characters and time taken to complete the loop to determine whether the character entered is correct or not. The power analysis attack is more complex and powerful in which the attacker observes the semiconductors' power usage during the clock cycles using an oscilloscope. This method can disclose passwords and cryptographic key to help the attacker gain physical access over devices.

IV.STANDARDS AND BASIC SECURITY PRACTICES

The cyber threat is evolving everyday with attackers developing new tactics to attack organizations. Staying informed and prepared to latest attacks and vulnerabilities can help the industry to prevent any loss or damage due to cyberattacks. In the new technological era, we have many practices and technologies that can help to achieve the knowledge about the vulnerable components of the manufacturing environment.

Vulnerability analysis is a process of discovering the weak points of an infrastructure that can contribute attackers with an entry point for exploitation of the whole infrastructure. Many vulnerability assessment professionals follow the process of checking basic compliance checks and vulnerability assessment processes followed by penetration testing to exploit those vulnerabilities and report the damage incurred by penetration testing.

The basic compliances are the set of documented established guidelines and standards that are needed to be followed by an organization to help them adhere to best security practices and proper handling of the sensitive data. Penetration testing is the process of exploiting the discovered vulnerabilities to check what information can an attacker get if the attack is carried out. It helps us to understand the attack framework and procedure and the data on threat if that attack occurs.

ISO/IEC 27001

An international and most basic standard that specifies establishment, implementation, maintenance of the ISMS (Information Security Management Systems). It includes guidelines for the risk management in an organization. The procedure includes major three steps- risk assessment, identifying security risks and implementing measures according to it.

NIST

National Institute of Standards and Technology or NIST includes a set of guidelines, best practices, and other standards for managing and improving cybersecurity. The core of NIST includes major 5 functions- Identify, Protect, Detect, Respond, and Recover.

CObIT

Control Objectives for Information and Related Technologies also known as CObIT is a framework developed by ISACA (Information Systems Audit and Control Association) for managing all the IT operations in an organization. Other security standards and frameworks such as PCI DSS, ISSAF, CREST also contribute to assessing the cyber risks.

4.1 Best Security Practices

Implementing security practices on every level in an organization is very important. It is often seen that people in organization often tend to make the infrastructure vulnerable at their end. By the time, the security experts reach the root of the problem, the damage is already done.

1. Managing patch updates and software updates for each system to protect systems from new vulnerabilities is necessary.
2. All passwords involved in the organization should be strong.
3. Authentication process should be at least two-factor.
4. Design a network architecture that includes segmentation to protect whole network from infected system.
5. Deploy network monitoring software and constantly monitor the network traffic for any anomalies.
6. Implementation of strong Encryption algorithm should be done to ensure secure data transfer over the network.
7. Keep up with new laws and standards to reduce risks and avoid lawsuits.
8. Employee training and awareness programs should be held regularly to ensure that each employee is aware of security practices like not downloading unknown file or clicking on malicious links.
9. Establish Zero-trust Architecture (ZTA) that include IAM and MFA to enforce least privilege access.
10. Sandbox should be implemented to ensure any downloaded file is not harmful for the system.
11. Implement SIEM (Security Information and Event Management) systems to analyse security events.
12. Risks assessment and management plan should be implemented to identify potential vulnerabilities and threats.
13. Incident response plan should be properly developed and documented to guide through procedures in the time of attack.
14. Physical security measures, i.e., securing the premises of the organization is also very important. Access control systems, surveillance cameras and its monitoring, guards and security staff all together contribute to securing the physical location of the organization.

V.ADVANCED TECHNOLOGIES AND SECURITY

The smart industry is focused on using advanced technologies to counter modern problems. The emerging technologies hold a great potential in the field of security. Furthermore, many technologies like AI and ML, blockchain are involved at greater extent in the security of smart manufacturing processes.

Machine Learning (ML) and Artificial Intelligence (AI) are critical technologies in enhancing the security of smart manufacturing environments. They provide advanced capabilities for detecting, responding to, and mitigating cyber threats, as well as optimizing operational efficiencies and safeguarding critical infrastructure. Security operations like anomaly detection and

threat identification, predictive maintenance, automated threat response, behavioural analysis of employees and users, etc. are based on several ML and AI techniques that build up the security of smart manufacturing industry.

Machine learning is an important part of a complex smart manufacturing environment. Many processes like anomaly detection, automated threat responses and IDS (Intrusion Detection Systems) work solely on machine learning and deep learning models. The ML techniques like ANN (Artificial Neural Networks), DNN, SVM, GAN are used to build the models on which the intrusion detection works [23].

By leveraging these technologies, manufacturers can proactively identify and mitigate cyber threats, ensure the integrity and security of their operations, and create a more resilient and secure manufacturing ecosystem. The integration of AI and ML into security strategies not only improves defence mechanisms but also enables more efficient and adaptive responses to the dynamic landscape of cyber threats.

Block chain is best described as a revolutionary technology that has many unique features such as immutability, transparency and decentralization which are capable enough to transform the of future technologies and practices. In simple terms, block chain is an immutable distributed decentralized digital ledger that keeps a record of all the transactions. The blockchain technology uses several encryption algorithms to make the transactions secure on a peer-to-peer network. In case of smart manufacturing, the block chain technology provides a secure, transparent, and tamper-proof infrastructure for data management, supply chain traceability, identity verification, and automated contract execution. Its ability to decentralize control and provide immutable records makes it a robust solution for mitigating various cyber threats and ensuring the integrity and security of manufacturing operations.

Block chain technology provides advantage of secure transactions, tamper-proof storage, and decentralized mechanisms for consensus. The paper [24], discusses a secure way to share resources over IoT devices in manufacturing environment using block chain. It provides low-cost technique for improving data security and privacy. The process of authentication is much secure and easier when implemented with block chain. The paper [25], describes permissioned block chain that allows limited access to the resources.

VI.CASE STUDIES

6.1 Honda Cyber-Attacks

Title: The Honda Cyber-Attacks

Introduction:

In 2017, a ransomware attack took place take made Honda's Sayama plant in Japan to shut down. This plant was infected by WannaCry ransomware that infected the production systems in the plant which resulted the production lines to drastically shut down for a significant time.

Then again in the year 2020, the Honda plant was under another ransomware cyberattack named EKANS (SNAKE). Honda was believed to be the first victim of this malware. This malware targeted the ICS.

Analysis:

Origin

The WannaCry ransomware was a cyberattack which was observed worldwide in 2017. According to Wikipedia [26], NSA (National Security Agency) developed a computer trojan called EternalBlue. This exploit was made to use as a defence mechanism against cyberattacks. It targeted a Microsoft vulnerability which was later fixed with a patch update by Windows. Unfortunately, this exploit was stolen by a group of hackers which they later used to target and infect Windows systems.

EKANS ransomware written in Go programming language targeted ICS operations. Dragos cybersecurity firm observed a malware in commercial malware repositories similar to EKANS in around late December of 2019 that targeted the ICSs. [27] It was discovered that it can infect Industrial Control Systems to implement the ransomware attack.

Target

The WannaCry targeted the systems that did not patch updated the Windows OS for SMB (Server Message Block) vulnerability. The EKANS targeted Industrial Control Systems (ICSs). ICS is the most essential part of the industrial environment as it controls and supports all processes in the manufacturing industry.

Technique

The WannaCry ransomware was a crypto ransomware that used an exploit that allowed them to control the system if it is connected to the same network. It starts by searching for the kill switch domain for the target. If kill switch is found it uses it to exploit the SMB vulnerability to spread itself to other systems connected to the same network. If the kill switch is not found it simply encrypts and locks the data on the current system, then moves towards exploiting the SMB vulnerability. Finally, they demand the ransom by displaying the message.

The EKANS malware was designed to target the ICS systems to shut down systems, encrypt the contents and demand the ransomware.

Impact

The WannaCry ransomware created a worldwide alarm affecting about 150 countries and infecting over 150000 systems. [28] It also affected the National Health Service hospitals in England and Scotland.

The EKANS ransomware attack at Honda manufacturing plant on June 9, 2020, greatly affected the production systems.

Although Honda has not specified which specific part of production was affected but it has publicly stated that many operations had to be suspended across the US, UK and Turkey causing a huge loss to the production company. [29]

Conclusion:

The lesson that can be learned from this is that system updates should be top priority in order to get latest security updates. Outdated systems are vulnerable to many cyberattacks that can cause serious impact.

6.2 German Steel Mill Attack

Title: German Steel Mill Cyberattack

Introduction:

In the year 2014, a steel mill was under cyberattack in Germany. The information about this attack was released by German government in which it was inferred that this was a result of a spear phishing attack. The attacker infested the ICS systems with malicious code hidden in a document send in an email. The code quickly escalated from the target system to the network to the mill plant. The report stated that multiple components of the ICS was affected which eventually leaded to failing of the sensitive and critical systems. The attack led to a massive physical damage to the steel mill plant. [30].

Analysis:

Technique

The attacker targeted some specific individuals to start with the spear phishing attack. The attacker made them to download the malicious file on their systems which initiated the attack.

In first stage, the attacker targets the system of the individual by exploiting the application vulnerability causing a remote connection to open. The lack of network boundary (Industrial Demilitarized Zone) caused the attacker to spread all throughout the network. In second stage of attack, the attacker has access to the network which allowed attacker to gather credentials and comprise small workstations then multiple components of ICSs leading the critical systems to shut down. The attack eventually caused a lot of physical damage in the steel mill.

Impact

As per the sources the impact of attack was mostly physical damage rather than intellectual theft or data theft. The disturbance with the ICS caused harm to the critical systems like Safety Instrumented Systems (SIS), HMI, Programmable Logic Units (PLC). The overall attack caused failure in regulation of blast furnace resulting that resulted in serious damage to the plant.

Conclusion:

The steel plant cyber-attack gave a lesson that even production and manufacturing environments are prone to attack if basic security practices are not followed. In this case, the lack of awareness and attention lead malicious files in the system. The network segmentation and demilitarized zone clearly failed or was not implemented that could have quarantined the system and not leading it to internal networks. Lastly, network monitoring or intrusion detection could have been helpful for the organization to know about intrusion in time and block or quarantine the infected system.

6.3 Stuxnet Worm Attack

Title: Stuxnet Worm Attack

Introduction:

In early 2010s, a team of cyber security experts discovered a cleverly designed worm. It was designed to target PLCs. The Stuxnet worm's main target was to attack ICS and PLC specifically from nuclear facilities.

Analysis:

Origin

The Stuxnet worm was believed to be developed jointly by Israel and United States as a part of "Operation Olympic Games". [31] This malware was designed to exploit the zero-day vulnerabilities to evade the security. In [32], it is mentioned that later on many variations of Stuxnet have been discovered such as Duqu and Flame. They used the source code of the Stuxnet worm and modified it to create an entirely new form of virus.

Technique

The technique used by Stuxnet was quite unique. It targeted the PLCs to infect them with malicious code and exploit rootkit functionalities. It also targeted Windows vulnerabilities to move within the network. The detection of this worm was made challenging as it used stolen digital certificates to appear as a legitimate software.

Impact

The Stuxnet worm has greatly impacted the industrial cybersecurity. It highlighted the weakness of the critical infrastructure of the industrial environment. It also raised concerns of misuse of cyber weapons to inflict physical damage on the property.

Conclusion:

The Stuxnet greatly raised the need of cybersecurity and collaboration of international governments to craft standards and develop strategies to face cyber threats. The basic security measures including regular software updates, network distribution and implementation of IDS is necessary to face such threats.

VII.DISCUSSION

The IT technologies build up the foundation for smart manufacturing industry and its security. The modern threats to the operational infrastructure can be mitigated using modern techniques and technologies. The analysis of these techniques and technologies for their scalability, feasibility and effectiveness in terms of security is discussed in this section.

Technology	Effectiveness	Feasibility	Scalability
Digital Twins	They provide security of actual physical systems in the manufacturing environment. Any incorrect command or unauthorised access to the systems is first reflected on digital twins and is blocked if required.	Very complex to design a good digital twin of a cyber physical system. Once implemented, it is easier to keep track and maintain using HMIs.	Scalability is a complex process and requires considerations of many factors.
AI and ML	These technologies provide wide range of uses in terms of security. They provide anomaly detection, behavioural analysis, predictive maintenance and much more.	Very easy to implement. It can work with almost every technology and serves different purpose with each one of them.	Highly scalable. Can enhance each technology it is integrated with. However, it may need different algorithms for each job.
Blockchain	The main purpose of blockchain in terms of security is to provide access control and supply chain security.	Highly complex architecture. Builds highly secured and trusted network.	Highly scalable but complex. Provides high security in terms of scalability.
Network Monitoring	Network monitoring tools provide a way to monitor and analyse the network traffic. It is integrated with machine learning algorithms to detect anomalies and alert or block any suspicious traffic. It helps to mitigate network-based attacks.	Very easy to implement and analyse. Highly effective and works better with ML techniques for better results. Automated responses associated with each activity can be easily implemented.	Scalability can depend on complexity of the network, network segments and traffic flow.
Zero Trust Architecture (ZTA)	ZTA ensures that each employee or person associated with the organization gets access to only the resources that are needed to complete their job.	Requires planning and high management skills to maintain access control lists (ACLs). Implementation is easy and is highly effective against insider attacks.	Easy to scale. Provides high security and privacy in terms of scalability.

Table 2. Comparison of different technologies and security method.

VIII.CONCLUSION

In conclusion, the security of smart manufacturing environment is a complex task that requires multiple level of security measures and regular checkups of security norms. Involving advanced technologies, when fully understood and exclusively picked according to the need of the organization, can help in securing the infrastructure. Each technology presents itself with its pros and cons. Thus, identifying the right combination of required technologies and security measures is more beneficial.

Although it is needed to be kept in mind that cyber security is a continuously evolving field with attackers constantly building new tactics trying to exploit new vulnerabilities. Blocking all future attacks is practically not possible. Hence, it is required to build a robust incident response plan to tackle with the attacks properly.

In general, implementing multiple security measures and constantly evolving with the threats is necessary. It is important to learn from past attacks and avoid attacks due to faulty security practices. It is important to realise that the attacker is constantly trying to find loopholes in security and impacts of attack on a manufacturing industry can lead to fatal accidents and far more serious issues than just data theft.

As smart manufacturing continues to evolve and integrate with emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain, it is imperative for organizations to stay vigilant and proactive in addressing cybersecurity risks and challenges. By adopting a comprehensive approach to cybersecurity, smart manufacturing organizations can effectively mitigate risks, protect against cyber threats, and realize the full potential of Industry 4.0 while maintaining the security and integrity of their operations.

REFERENCES

1. *1M. Grieves, Digital Twin: Manufacturing Excellence Through Virtual Factory Replication, White Paper, 2015, Online: https://www.3ds.com/fileadmin/ PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-DigitalTwin-Whitepaper.pdf -03-01)*
2. *2M. Attaran, S. Attaran, Collaborative supply chain management: The most promising practice for building efficient and sustainable supply chains, Bus. Process Manag. J. (2007)*
3. *3Y. Blomkvist, L.E.O Ullemar Loenbom, Improving Supply Chain Visibility Within Logistics by Implementing a Digital Twin: A Case Study at Scania Logistics, KTH Institute of Technology, Stockholm, Sweden, 2020*
4. *4Z. Kang, C. Catal, B. Tekinerdogan, "Remaining useful life (Rul) prediction of equipment in production lines using artificial neural networks", Sensors 21 (2021) 932*
5. *5Dassault Systems, the living heart project, 2022, Online: https://www.3ds.com/ products-services/simulia/solutions/life-sciences-healthcare/the-living-heartproject/*
6. *6K. Subramanian, Digital twin for drug discovery and development—The virtual Liver J, J. Indian Inst. Sci. 100 (4) (2020) 653–662.*
7. *7M. Xiong, H. Wang, Digital twin applications in aviation industry: A review, Int. J. Adv. Manuf. Technol. 121 (9–10) (2022) 1–16*
8. *8 Y. Chen, "Integrated and Intelligent Manufacturing: Perspectives and Enablers," Engineering, vol. 3, pp. 588–595, Oct. 2017*
9. *Z. Liu, N. Meyendorf, and N. Mrad, "The role of data fusion in predictive maintenance using digital twin," in Annual Review of Progress in Quantitative Nondestructive Evaluation, (Provo, Utah, USA), p. 020023, 2018*
10. *Y. Zheng, S. Yang, and H. Cheng, "An application framework of digital twin and its case study," Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 1141–1153, June 2018*
11. *R. Vrabič, J. A. Erkoyuncu, P. Butala, and R. Roy, "Digital twins: Understanding the added value of integrated models for through-life engineering services," Procedia Manufacturing, vol. 16, pp. 139–146, 2018*
12. *A.Madni, C. Madni, and S. Lucero, "Leveraging Digital Twin Technology in Model-Based Systems Engineering," Systems, vol. 7, p. 7, Jan. 2019*
13. *Tao, Fei, Meng Zhang, and Andrew Yeh Chris Nee. Digital twin driven smart manufacturing. Academic press, 2019*
14. *T. Bergs, S. Gierlings, T. Auerbach, A. Klink, D. Schraknepper, T. Augspurger, The concept of digital twin and digital shadow in manufacturing, Procedia CIRP 101 (2021) 81–84*
15. *J. Davis, Nat. Sci. Foundation, Workshop Proceedings on Cybersecurity in Chemical and Biological Process Systems: Impact and Directions 2006*
16. *DIN VDE The German Standardization Roadmap for Industrie 4.0 Version 1.0. 2014 https://www.din.de/resource/blob/65354/1bed7e8d800cd4712d7d1786584a7a3a/roadmap-i4- 0-e-data.pdf*
17. *M. Hannah, M. James, S. Johnson, C. Leiva, A. Michel, D. Noller, F. Riddick, D. Riley, E. Wallace, B. Williams, Interna- tional. 2016 https://www.pathlms.com/mesa/courses/14866*
18. *Y. Lu, K. C. Morris, S. Frechette, NIST 2016 https://nvipubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf*
19. *Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions, Computer Communications, Sri Harsha Mekala, Zubair Baig, Adnan Anwar, Sherali Zeadally, https://doi.org/10.1016/j.comcom.2023.06.020*
20. *Wikipedia, "Purdue enterprise reference architecture," https://en.wikipedia.org/wiki/Purdue Enterprise Reference Architecture, 2019.*
21. *N. Jiang, H. Lin, Z. Yin and L. Zheng, "Performance Research on Industrial Demilitarized Zone in Defence-in-Depth Architecture," 2018 IEEE International Conference on Information and Automation (ICIA), Wuyishan, China, 2018, pp. 534-537, Doi: 10.1109/ICInfA.2018.8812486.*
22. *MITRE CVE records (Online) Case ID: CVE-2007-3108 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3108*
23. *Alotaibi, A.; Rassam, M.A. Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defence. Future Internet 2023, 15, 62. https://doi.org/10.3390/fi15020062*
24. *Tan, Jinbiao, Jianhua Shi, Jiafu Wan, Hong-Ning Dai, Jiong Jin, and Rui Zhang. "Blockchain-Based Data Security and Sharing for Resource-Constrained Devices in Manufacturing IoT." IEEE Internet of Things Journal (2024).*
25. *Ciampi, Mario, Diego Romano, and Giovanni Schmid. "Process Authentication through Blockchain: Three Case Studies." Cryptography 6, no. 4 (2022): 58.*
26. *EternalBlue - Wikipedia*
27. *Dragos "EKANS Ransomware and ICS operations" https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/#_ftn1*
28. *WannaCry ransomware attack - Wikipedia*
29. *"Honda Shuts Down Factories After Cyberattack" https://www.popularmechanics.com/technology/security/a32825656/honda-cybersecurity-attack/*
30. *Lee, Robert M., Michael J. Assante, and Tim Conway. "German steel mill cyberattack." Industrial Control Systems 30, no. 62 (2014): 1-15. https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf*
31. *Ellen Nakashima, Greg Miller & Julie Tate, U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say, WASH. POST (June 19, 2012), https://www.washingtonpost.com/world/national-security/us-israel developed-computer-virus-to-slow-iranian-nuclear-efforts-officials say/2012/06/19/gJQA6xBPoV_story.html.*
32. *Lawrence J. Trautman and Peter C. Ormerod, Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things, 72 U. Miami L. Rev. 761 (2018): https://repository.law.miami.edu/umlr/vol72/iss3/5*