American Journal of Artificial Intelligence and computing

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

AI and Cybersecurity in Smart Manufacturing: Protecting Industrial Systems

Shah Zeb[1], Shahrukh Khan Lodhi[2*]

[1]Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria, VA

[2]Trine University Detroit, Michigan

[1]szeb.student@wust.edu, [2]slodhi22@my.trine.edu

open access

Corresponding Author

Shahrukh Khan Lodhi
slodhi22@my.trine.edu

Article History:
Submitted: 12-01-2025
Accepted: 07-04-2025
Published: 07-04-2025

Keywords:
AI-driven cybersecurity, automation, business continuity, cyber threats, defense-in-depth, Industrial IoT (IIoT).

ABSTRACT

Limited industrial system security occurs due to fast industrial machinery unification with AI and IIoT devices and automation systems for intelligent production spaces because hackers leverage these targets to infiltrate malicious code while also gaining access to sensitive information. This research assesses how security mechanisms which unite AI with Zero Trust Security principles combine defense-in-depth methods for protecting industrial production sites against threats. When AI detects security threats right away it automatically starts security protocols for manufacturers to stop digital attacks before they begin. Companies achieve maximum protection when they secure their IIoT equipment and create network segmentation and MFA implementation. Company security success emerges when dedicated employees support protective security systems that are consistently developed for their needed purposes. Studies from recent times demonstrate that organizations which create dependable incident response plans and maintain continuous business continuity alongside employing modern cybersecurity policies achieve secure industrial system outputs. The security system needs AI components that manufacturers must create to safeguard their industrial networks against cyber threats in this digital age.

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

INTRODUCTION

Smart Manufacturing stands as the main driver of production change because digital advancements thrive to advance manufacturing practices. The combination of IIoT technology with AI big data analytics cloud computers and advanced technology enables companies to establish better production techniques while improving reliability at their industrial facilities. Implementing professional security measures becomes necessary for industrial systems because the convergence of crucial benefits and significant risks stemming from field-based technological advancements [1]. Industrial production functions as a result of digital technologies as well as collected information through the framework of Smart Manufacturing. The combination of sensors working with automated systems and AI and real-time data processing systems enables organizations to reach peak factory operations. The automatic design of smart manufacturing systems achieves enhanced results by enabling automatic operation adaptation and production optimization due to their non-static sequence procedures [2]. Several operational components must exist for a factory to operate as a smart facility.

The processing of performance metrics by AI systems allows them to forecast potential problems thereby developing superior strategic choices. The use of AI-based robots leads to improved speed capabilities and performance enhancement resulting in higher precision during task completion. Businesses deploy cloud along with edge systems to process data which boosts their speed of business response. These features result in enhanced manufacturing profitability and establish multiple security points which hackers can easily leverage to conduct their attacks [3].

CYBERSECURITY CHALLENGES IN SMART MANUFACTURING

Manufacturers need to establish robust cybersecurity measures for operations which integrate AI and IIoT functions. When proper connection integration occurs between operational systems it creates security vulnerabilities because this method establishes entry points through which hackers can access both private information and disrupt operations. Three distinct cybersecurity issues affecting smart manufacturing operations have been discovered [4]. IIoT demands interconnected factory networks which was not necessary during previous manufacturing operations. Network security requires absolute protection from all attacks because hacker attacks become more numerous when entrypoints increase significantly. Critical IP information combined with operational data inside smart manufacturing systems exposes them to attacks from ransom ware encryption programs and unauthorized access by cyber spies. The combination of ransom ware leads to system immobilization

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

but industrial espionage results in the acquisition of valuable business intelligence for strategic purposes [5].

Figure: 1 showing challenges of cybersecurity in smart manufacturing

Businesses across industries need to handle security risks within their production systems since those systems were developed before widespread internet adoption. Outdated systems pose direct security risks because industries failed to supply critical updates which should be performed on their systems. Network protection operates alongside AI systems because cybercriminals execute advanced automated hacking operations through the use of AI technology. Manufacturing companies require AI-based security solutions to counter newer sophisticated threats that emerged from AI developments. Smart manufacturing faces its main security challenges from internal system issues rather than external intruders together with basic human mistakes. A large number of threats arise from manufacturing personnel who misuse authorized access and break workplace rules or make accidental errors [6].

AI technology deployment provides better security for smart manufacturing by addressing operational security problems and protecting data safety. Security risks are noticed promptly by the system preventing cyber-attacks from causing operational damage. The automatic systems must become instantly active whenever attacks take place. Behavioral profiling methods need to be utilized

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

for creating advanced security defense systems. AI cybersecurity protection implementation for smart manufacturing systems is now required due to its dual role in preventing cyber-attacks and maintaining operational sustainability according to [7].

THE ROLE OF AI IN SMART MANUFACTURING

The paradigm of fundamental production lines undergoes alteration through Artificial Intelligence because it supports the development of automated systems that operate independently to boost production effectiveness. Operations in industry receive enhanced efficiency through the combination of deep learning technology and machine learning and computer vision which helps produce better equipment predictions and actionable decisions. Manufacturers can produce better products with the help of AI while AI also reduces production delays and strengthens their supply network security and delivery services [8].

The greatest manufacturing achievement of AI results from its ability to link autonomous systems with robotic operations. AI systems perform repetitive accurate tasks throughout production to simultaneously produce more products and guarantee human safety within the working environment. These systems: The automated computer vision system of our production line conducts immediate quality checks during defect detection operations. Producers need technology to allow robots interact safely with humans during operations. The implementation of AI systems enables organizations to make sound choices about production product modifications. Through their installation at manufacturing facilities man-made intelligent systems enhance operational capacity and simultaneously minimize output defects and waste material production to deliver stable finished products [9].

Predictive Maintenance and Equipment Optimization: Unplanned stoppages caused by scheduled maintenance checks along with prompt repairs directly result in financial losses for factories. By employing predictive maintenance AI operates through analyzing sensor data and algorithmic predictions to find equipment problems [10]. The system provides preliminary signs indicating equipment breakdown before it reaches critical states. Using our system enables personnel to detect equipment breakdowns before these situations materialize in reality. Better maintenance procedures need to be implemented by our organization to minimize asset unavailability occurrences. Real-time equipment data processing by AI systems helps increase operational availability besides lowering service expenses and boosting system performance [11].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

AI-Driven Supply Chain and Inventory Management: Thorough supply chain operation enhancement comes from AI-enabled data analysis that generates optimized order management alongside reduced inventory storage which results in decreased material loss. Manufacturers benefit from smart algorithms when these systems help them track market fluctuations to sustain suitable production rates between markets' supply and demand. The system requires capabilities for procurement operations to support smooth time-based delivery of materials. Our system will discover innovative methods to organize delivery routes together with cost-efficient product transports. From analyzing real-time big data AI enables power companies to gain superior control over their supply networks that allows quick market adaptation. [12]

AI IN QUALITY CONTROL AND DEFECT DETECTION

The improvement of manufacturing quality through Artificial Intelligence occurs by implementing these methods. A product testing system with advanced computer vision functions as a solution that boosts both speed and accuracy in problem detection. The systematic flaw identification process of machine learning models leads to proposed factory development solutions. Our automated system prevents abnormal data from harming our manufacturing quality through advanced detection capabilities. With their ability to detect errors AI systems decrease manufacturing defects which in turn leads to increased customer satisfaction from products of better quality [13]. AI provides cyber defense for smart factories through its ability to detect abnormal network operations while simultaneously identifying current threats. AI security analytics provides the ability to identify and prevent cyber-attacks from happening yet to take place.

The system our team operates allows security risks to be identified in advance which subsequently leads to risk blocking that protects our systems. Manufacturers can shield their confidential data and maintain system security through AI-based protective methods. The implementation of AI in smart manufacturing leads to superior operational performance as well as enhanced decision-making capabilities which ensures operational protection [14]. The progression of AI technology allows organizations to combine production maintenance systems and enhanced security protocols which leads to better business performance outcomes plus digital market protection. AI will possess greater control over industrial operations to secure them in the forthcoming years as its advancements continue [15].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

CCI devices and cloud-based platforms and automated AI systems allow smart manufacturing development to enhance connections between industrial systems. Modern advanced technologies provide enhanced performance although they create fresh cybersecurity threats in the process. Industrial system cyber-attacks lead to facility production delays which require money and data costs and result in physical asset damage. Knowledge of current cybersecurity risks enables proper protection for industrial sites [16]. The current era of production systems encounters significant cybersecurity threats because attackers seize control of these systems to extort ransom payments for their system release. After taking control of vital information the attackers demand ransom money for its release. The interruption of ICS networks along with SCADA devices creates substantial danger because it results in the complete shutdown of every industrial production line. Recent history shows that multiple manufacturers endured ransom ware attacks according to documented reports [17].

Processing systems fail to operate unless the hackers receive their demands leading to total production destruction. Business operations experience negative impacts from encrypted design or operational data that falls into hacker control. The performances of supply chains suffer damage when cyber attackers take over delivery management systems and inventory control infrastructure [18].

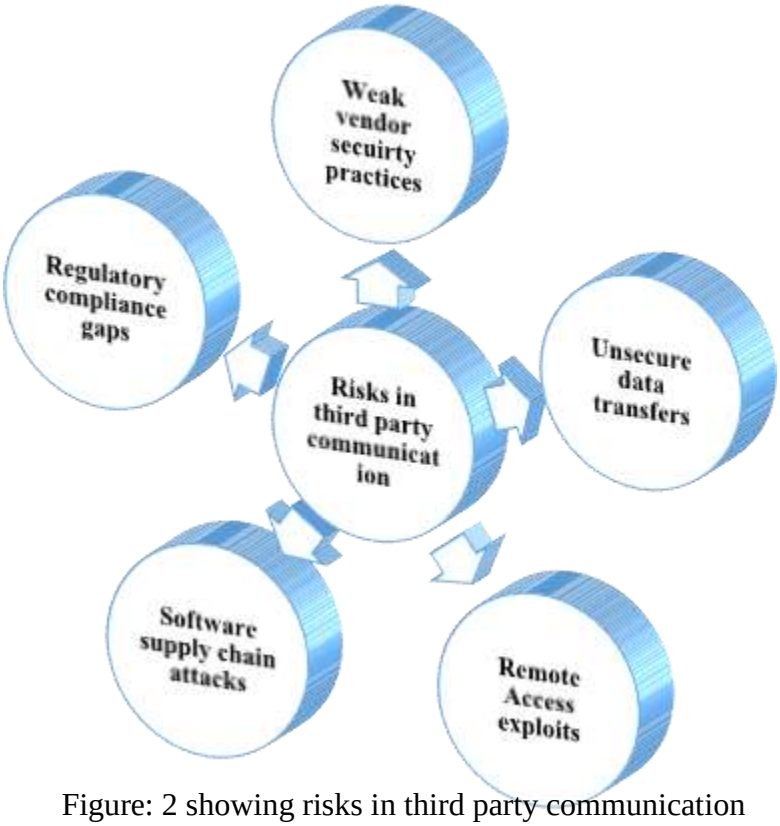

Figure: 2 showing risks in third party communication

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

Manufacturing organizations protect their intellectual property materials composed of product designs and trade secrets and proprietary technologies on their computer systems. Business data which holds importance to companies becomes the target of cybercriminals as well as other organizations through fake email communications and computer infections. They also appear legitimate. Natives who work within company networks assist outside hackers as they obtain confidential data. Business success undergoes reduction due to product secret theft by cybercriminals. Theft of valuable technology by competitors results in monetary losses because these same competitors can launch into the market using stolen data. When trust between customers and investors decreases your organization will face negative reputation consequences [19].

Supply Chain Attacks

Smart factories which partner with external organizations become susceptible to supply chain attacks because of their relationships with external organizations. The main manufacturing system becomes accessible to attackers because they capitalize on weak security measures throughout supplier networks. External software and firmware downloading platforms frequently deploy dangerous system updates for deployment. The exploitation of infected Internet of Things devices results in system security breakdowns for hacking purposes. When service privileges are transferred improperly an unauthorized person can gain complete control over our system [20].

Insider Threats and Human Error: Most cyber dangers come from outside the organization yet attacks caused by internal agents can lead to severe harm. Workers who want to cause damage to their company and staff members and system maintenance personnel from external organizations create the greatest security threats. The primary signs of insider security threats comprise the deliberate attempts to damage manufacturing production systems. Accidental sharing of sensitive information due to phishing or social engineering attacks. The lack of secure password control systems lets hackers obtain unauthorized system entry [21].

AI-Powered Cyber Attacks: AI systems deployed for security grow at a similar rate as attackers enhance their methods by using AI technology. The evasion techniques learned by malicious code allow it to bypass security system protections. Our system generates focused phishing communication which succeeds in tricking more users effectively. Security vulnerabilities become detectable to AI systems before manual security checks can trigger appropriate responses by teams [22]. Smart manufacturing security environments experience rapid changes which have led hackers to develop

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

attacks that use both ransom ware and AI-involved digital assaults. Defects in security measures lead organizations to accept financial losses while facing operational interruptions and preventing access to their data assets. Manufacturers need to incorporate AI security tools which enable access control while identifying threats on a regular basis to protect their operations from digital dangers [23].

AI-DRIVEN CYBERSECURITY SOLUTIONS

The escalating security threats throughout Smart Manufacturing operations make traditional protection methods inadequate for shielding Industrial Control Systems (ICS) devices and IIoT equipment together with production network cloud infrastructure. Modern cybersecurity systems fight cyber threats using AI behavioral learning models which monitor network traffic and thus generate quick responses to potential attacks [24].

The protection of smart manufacturing relies primarily on artificial intelligence to swiftly locate and detect unexpected network operations. Data security systems leverage AI detection to examine network feeds as well as user behavior and system logs in order to detect potential cyberattacks. AI systems possesses the ability to detect hidden dangerous activities that traditional security devices cannot identify. The system detects irregularities which happen during machine operations and user activities to identify possible insider security risks [25]. The system processes security information at a speed humans cannot match. AI threat detection offers security personnel the capability to discover potential dangers at earlier developmental stages so major losses can be prevented. Machine learning programs use analyzed past attacks to detect threats that help identify probable future cyber-attacks [26]. This allows manufacturers to:

Your company should enhance security functions which require improvement actively. The system establishes procedures both to find potential security threats and to automatically overcome them before they occur. Security problems should be prevented from disabling your business operations temporarily while also costing you money through security breaches. The predictive analytics algorithms notify organizational entities about future cyber risks to help them improve their protective measures. The security technology benefits from artificial intelligence because it implements instantaneous responses when threats are detected and their resolution process starts simultaneously. The automatic detection of security threats with AI systems operates independently until human staff can intervene [27].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

The system performs instant segmentation of infected devices as malware can migrated across the network. Through our security system we deliver instant updates which protect exposed system parts. The network reacts by blocking suspicious IP addresses while discontinuing any unauthorized access to the system. The quick detection capabilities of AI security solutions decrease the response time toward cyber threats that makes them less dangerous. The smart manufacturing security system receives support from AI which enables system access control through its features. A better form of user authentication together with restricted entry for unapproved people enables AI to offer superior data protection [28].

The operational capabilities of systems enhanced by AI help identify and prevent unauthorized login actions that aim to tamper information. The combination of facial recognition with fingerprint scanners serves as the main component of our security defense systems. The security system adjusts user access permissions following the identification of security risks. AI controls manufacturing access systems for authorized factory personnel with its operational framework. Additional businesses deploying IIoT devices together with cloud systems have intensified their exposure to hacker threats [29]. AI tools protect natural spaces because they perform these security-enhancing activities. The system tracks current device connections to locate strange activity patterns. Security encryption is embedded into our system to create protection for industrial data from unauthorized access. Modern systems need detection of security flaws discovered in IoT software together with their connected programs [30].

An AI-based protection system safeguards cloud and IIoT technologies to allow smart manufacturing operations under high security with minimal hacker interference. The modern industrial environment gets automated cybersecurity protection which delivers instant responses to detected security threats. AI systems identify potential security threats in advance to activate automated security blockers that defend vital manufacturing data from unauthorized intruders. Manmade security systems require artificial intelligence protection since cyber threats progress steadily each day [31].

THREAT DETECTION AND ANOMALY IDENTIFICATION USING AI

Cyber attackers now use more complicated and frequent methods that avoid traditional security the organization implements various approaches to secure its smart manufacturing system. Security teams defend their Industrial Control Systems ICS and Industrial Internet of Things IIoT equipment against threats by detecting them when they happen through modern AI-influenced security systems

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

that examine abnormal behavior patterns for preventive measures [32]. Security systems based on AI technology surpass pre-established threat scanning by delivering instantaneous detection of abnormal activities. Security platforms operate today struggle to detect all zero-day threats along with new malware since their detection methods are no longer efficient against the latest hacking techniques. Security systems gain strength through ML and deep learning technology because these systems analyze security data to identify abnormal patterns [33].

Artificial intelligence enhances aerodynamic capabilities of airplanes through wiser designs and more efficient operations and improved aerodynamic function. Through neural networks and machine learning technology wind turbine and airplane aerodynamic design cycles experience speed boosts and their computational costs decrease [34]. Aerodynamic forecasts are generated when vortex lattice methods are joined with high-fidelity simulations then used to produce 3D-printed models that can move directly into practical applications and wind tunnel-tested results [35]. Point cloud analysis with surface deviation assessments enables the development of more precise design validation methods since they enhance accuracy quantification techniques. Companies use artificial intelligence systems coupled with computational tools to create experimental procedures which generate new sustainable high-performance aerodynamic systems [36].

The system finds and blocks new malware types through observing system processes which helps detect established patterns. The security system extends its protection for both known and unknown risks because it constantly studies and adjusts its operational functions. AI takes unprocessed data to create security information which gives immediate safety alerts through continuous network traffic monitoring for suspicious activities. Malware detection causes the system to identify infected devices that receive automatic blocking prevention for spreading malware. Security systems which are respond able detect and automatically raise alarms about all security threats [37].

The early response system decreases response time while stopping major system failures from occurring. The vulnerability detection features of artificial intelligence allow smart manufacturing systems to achieve self-protection against cyber dangers. AI algorithms use processing methods to protect systems from security threats which both disrupt operational activities and allow thieves to steal intellectual property. AI cybersecurity becomes mandatory for implementation because of evolving cyber threats [37].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

SECURITY MEASURES OF INDUSTRIAL INTERNET OF THINGS (IIOT)

The IIoT technology links industrial equipment to sensors with controllers leading to enhanced asset management features that produce real-time decision possibilities. IIoT technology functions through multiple security risks which exposes its devices to easy hacker access. The protection of both IIoT systems and their attached devices remains crucial because it ensures the basic functions and operational safety of industrial complexes. IIoT systems endure multiple security problems since they unite modern technology architectures with legacy equipment that remains challenging to protect [38]. The major security risks include:

The basic security capabilities along with old software packages and accessible passwords found on IIoT devices enable attackers to exploit them at great speed. Industrial operations experience damage due to internet hackers when they gain unauthorized control of unsecured IIoT devices. The industrial information from IIoT devices attracts cybercriminals because these attackers exploit the devices to steal important records. The hijacked IIoT devices enable cybercriminals to launch substantial Distributed Denial-of-Service (DDoS) attacks that break production systems. Strong artificial intelligence security tools represent the most effective security solution for IIoT environments requiring installation by industries [39].

AI improves IIoT security via instant threat detection while creating automatic responses that monitor abnormal activities and security threats. Primarily secure systems develop their foundation through artificial intelligence technology. The system employs AI to track both IIoT network data flow together with device behavior patterns that allow it to detect potential security risks. The monitoring system employs AI technology for detecting uncommon device activities as it performs its surveillance functions. Unusual data transmissions to unknown servers. Unauthorized device access or sudden changes in system configurations. Criminal gadgets distribute computer viruses through their implementation of malicious software [40]. The analysis of abnormal behavioral patterns by AI security systems enables automated preventive measures which prevent incidents from escalation. Security systems become more effective because AI develops methods to authenticate users while inspecting devices prior to access approval. The system authorizes user access through biometric body measurement such as face or fingerprint scans. Computer systems use this technology to recognize abnormal activities between users and devices through monitoring their behavioral patterns. RBAC rules determine employee access rights which prevents internal security problems [41].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

The security system provides secure connection access between authorized users and devices to reach valuable operational equipment. IIoT networks become endangered by regular firmware updates and system patches. The system deploys AI to identify obsolete firmware after which it initiates installation tasks. The system needs to identify potential security risks before hackers can use them. Patches are automatically installed to protect operational activities because security risks manifest so security operations can continue without disruption. IIoT devices gain defense against contemporary threats because they receive automatic firmware updates [42]. Secure connections between IIoT devices must be safeguarded because the devices constantly exchange information during operations. AI-driven security measures help:

The system carries out secure data transfers by implementing secure cryptographic channel protocols along with advanced security features. The system detects modifications in data records in order to identify unauthorized access attempts and data manipulation. An IIoT platform needs block chain integration to establish data security against unauthorized modifications in data communications. According to the Zero Trust Security Model every device and user requires advanced protection controls to be verified before receiving trust. The implementation of AI improves Zero Trust by conducting continuous assessments of IIoT system identity verification and activity details for industrial network protection [43]. Access to the system is provided only when effective safety tests show present conditions meet security requirements. The company needs to identify and prevent corporate users who want to damage industrial cybersecurity systems. Secure practices for IIoT devices and connected systems stop cyber-attacks that target smart manufacturing plant operations. The real-time surveillance provided by AIs security systems together with automated defense strategies enhances safety and access control for industrial equipment and thus promotes the adoption of IIoT systems [44].

BEST PRACTICES FOR CYBERSECURITY IN SMART MANUFACTURING

By employing AI-based networks for smart manufacturing operations success becomes attainable since cybersecurity must always maintain its position as the primary focus with every part and system involved. Data theft attempts against industrial systems and attacks on production networks and IIoT devices cause network destruction and data corruption which leads to profitability decline and operational disruptions. Security solutions for manufacturers must combine artificial intelligence-based defensive systems with human security personnel who both identify threats and deal with upcoming safety risks [45]. Every network device and system and user has to establish their validity

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

as a prerequisite to gain entry under a Zero Trust Architecture. The protection strategy bases its security efforts on centralized rules which serve as barriers against unauthorized entry.

Key Zero Trust principles include:

Every user or device must obtain access permissions that match their job requirements.

Require multiple authentication methods for access. The system applies artificial intelligence technology to detect abnormal user activity patterns while watching all user actions. Micro-Segmentation: Isolate critical systems from less secure parts of the network [46]. Zero Trust Security acts as a manufacturing defense system which protects network systems from security intrusions by blocking unauthorized access while detecting threats in an early stage. Artificial intelligence-based security tools inspect real-time data collection to detect security risks before standard control systems become effective. To achieve maximum AI security benefits a company must implement this system: This program combines user activity data with network behavior evaluation to identify performance changes beyond standard business operations [47].

Automatic security systems based on AI protect breached systems before activating defense protocols. The implementation of machine learning by security systems examines security risks to identify potential cyberattacks before they initiate. Better protection of systems can be achieved by cyber defenders who integrate intrusion detection AI systems with SIEM tools which observe security trend developments. The high frequency of hacker attacks on IIoT devices creates the necessity for protection [48]. Firms should maintain constant firmware updates for their IIoT devices to keep them secure because this is a critical requirement for establishing good Industrial Internet of Things security principles. A different set of credentials and certificate-based authentication should be implemented for every IIoT device. The network performs end-to-end encryption of industrial data to guarantee safe transmission [49].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

Figure: 3 showing security measures based on a zero trust approach

You should isolate IIoT devices into separate network segments so hackers cannot jump between network domains. Manufacturers should test their security position through repeated assessments which include: Our team performs cyberattack replication to reveal potential weakness in your system. Security measures undergo evaluations to ensure their compliance with NIST as well as ISO 27001 and IEC 62443 official business frameworks. The team conducts pro-active checks for possible security threats that exist within industrial network systems [50]. Threat evaluations conducted by organizations reveal security vulnerabilities which guide increased protective measures to prevent potential attacks from cybercriminals.

The integration of employee security training into business operations will decrease the frequently encountered cybersecurity failures caused by employee mistakes. Workers need training since it enables them to identify deceptive online practices in emails and security system manipulation methods. The correct security measures must be fully implemented to safeguard personal information. Use complex security passwords which should also activate secondary authentication protocols while accessing personal accounts [51]. Poisonous situations should prompt employees to call IT security

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

without delay. Employee training represents the primary defense measure which protects organizations from cyber threats. A dependable backup system represents the best strategy to handle cyber-attacks because it restores operations quickly [52]. Best practices include:

An organization should protect its essential data by maintaining backup storage on offline devices and employing encrypted cloud space storage. The organization needs to determine along with its employees the fastest practices to manage security breaches. Your company needs to implement AI defense systems which identify ransom malware attacks for blocking purposes. The testing of disaster recovery procedures creates conditions where manufacturers start normal production activities right after experiencing cyber incidents. For protection against cyber threats smart manufacturing systems require advanced AI-defense solutions which should be installed at various entry points. Manufacturers maintain protection of their industrial networks through Zero Trust Security alongside AI protection systems and IIoT security controls and staff training protocols. Our smart manufacturing system has to maintain security through planned assessments and tests of security protocols and threat evaluations coupled with emergency readiness preparedness [53].

Smart manufacturing developments which link AI technology with other innovations have generated new cybersecurity challenges that prove difficult to solve. Modern industrial cyber threats consist of three components: network intrusions, targeted attacks on vendor-supplied products and attacks on connected devices. Smart manufacturing operations receive two main safety benefits from automated threat anticipation and AI-based system testing which develops equipment defense against cyber-attacks [54].

SECURITY SYSTEMS USING AI TECHNIQUES

Records from past cyber-attacks need evaluation to determine future threats which security crews need to intercept at their onset. Machine learning algorithms automatically discover cyber-attacks in order to stop their evolution toward operational infrastructure. Cybersecurity systems need self-operating functionality which also includes threat detection abilities for newly appearing security vulnerabilities. By employing AI predictive analytics industry manufacturers obtain the capacity to discover cybercriminals before reactive security measures detect attacks [55]. Future cybersecurity systems require independent AI security agents to operate autonomously for detecting threats immediately after their detection. The system implements automated procedures which fix its internal network weaknesses [56].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

Real industrial conditions replicated by AI technologies serve as testing grounds for hackers allowing analysis of their expertise. Automatic safety functionality activation will decrease incident response periods thereby allowing manufacturers to combat high-level cyber threats more effectively. The ability of quantum computers to protect smart manufacturing networks faces challenges in terms of both technical barriers and beneficial features against cyber threats. Quantum computer-based encryption advancements have established security points of failure which manufacturers need to replace with different security systems [57]. To counter this, manufacturers must:

You should start deploying encryption methods which resist quantum attacks before such threats lead to substantial damage. The implementation of quantum-resistant AI programmed defense systems should protect and observe industrial networks. Manufacturers need to establish strategies using future-generation encryption to preserve their industrial data systems. Manufacturers face rising cyber threats because they rely on their third-party vendors who operate supply chain operations through cloud-based services [58]. The protection of supply chains through AI systems will happen through these activities:

Identifying vulnerabilities in supplier networks. The system supports identifying defective parts which are currently utilized during production operations. The system provides real-time visibility of entire supply chain operations to enterprise users. AI security systems will perform automatic source connection sweeps for threats which trigger immediate stoppage to avoid factory disruptions. Smart manufacturing receives protection from AI through advanced security detection models which employ self-operating systems and combine block chain protection with quantum security and artificial intelligence for supply chain protection. Manufacturers require AI-driven cybersecurity systems to implement defensive measures for their industrial operations in compliance with rules to build security infrastructure for manufacturing of the future [59].

Better cyber incident response capabilities emerge in manufacturers who implement AI systems. A business will not gain maximum security even with perfect systems until workers understand threats and receive needed training. Resilient employees need to learn about social engineering techniques used by phishers for attack recognition. The protection of your system requires both strong passwords and always updated software along with ongoing basic security practices maintenance. Staff members in IT security should get alerted about abnormal system activities to start their investigations swiftly [60].

ISSN : XXXX-XXXX
Volume 1, Number 1, 2025

Security training builds employee abilities to help defend industrial plants and systems. A reliable smart manufacturing cybersecurity plan needs to protect business operations from attacks but also enable operations to survive and bounce back after cyber incidents. Manufacturers will achieve total security by combining AI cybersecurity solutions and comprehensive defense systems with staff up skilling [61].

CONCLUSION

As smart manufacturing transforms further through AI and IIoT technologies it creates stronger security needs to protect connected operations. Industrial systems connected to broader networks make them vulnerable to multiple cyber dangers such as malware infections, hacking attempts and cyber theft. AI security needs must have multiple resistances that combine to safeguard operations and data security.

AI enhances cybersecurity by monitoring threats instantly while predicting threats and taking swift response actions. AI-based systems automatically find and block threats early to keep networks secure through consistent monitoring and reaction to unusual activities. Zero Trust Security model plus defense-in-depth techniques and IIoT security systems work together to shield industrial networks and their connected devices.

While technology tools are vital our response depends on skilled personnel and staff with security knowledge. Organizations need to train their staff about social engineering threats along with the correct ways to handle phishing attacks and secure their work habits. An educated workforce stops most cyber threats from entering your system through human error. Manufacturers build strong recovery tools to handle attacks promptly and keep operations running smoothly. Regular checks of security systems find weaknesses that need improvement to stop hackers before they attack.

Moving forward cyber-security for smart manufacturing depends on AI-based protection system automation as well as quantum encryption and AI threat detection throughout supply chains. To protect their operations against changing cyber threats manufacturers need to use new security tools and support new industry standards while regularly strengthening their security system. To succeed in smart manufacturing businesses need to recognize that strong cybersecurity exists as both a protective technology and a strategic requirement. Using AI security systems and best cybersecurity measures with proactive defenses will keep manufacturers safe and create dynamic smart manufacturing networks.

REFERENCES

[1]. Mijwil M. M., Doshi R., Hiran K. K., Al-Mistarehi AH, and Gök M., "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," Mesopotamian journal of cybersecurity, vol.2022, pp:1-4, January 2022. https://doi.org/10.58496/MJCS/2022/001

[2]. Bibby L. and Dehe B., "Defining and assessing industry 4.0 maturity levels – case of the defence sector," Production Planning & Control, vol.29, no.12, pp:1030-1043, September 2018. https://doi.org/10.1080/09537287.2018.1503355

[3]. Bala I, Mijwil MM, Ali G, Sadıkoğlu E. Analysing the connection between AI and industry 4.0 from a cybersecurity perspective: Defending the smart revolution.

[4]. Atal DK, Tiwari V, Kumar D. Recent Advances in Cybersecurity in Smart Manufacturing Systems in the Industry. Handbook of Smart Manufacturing. 2023 Jul 17:41-62.

[5]. Shrivastava A., Krishna K. M., Rinawa M. L., Soni M., Ramkumar G., and Jaiswal S., "Inclusion of IoT, ML, and Blockchain Technologies in Next Generation Industry 4.0 Environment," Materials Today: Proceedings, vol.80, no.3, pp:3471-3475, 2023. https://doi.org/10.1016/j.matpr.2021.07.273

[6]. Hoosain M. S., Paul B. S., and Ramakrishna S., "The Impact of 4IR Digital Technologies and Circular Thinking on the United Nations Sustainable Development Goals," Sustainability, vol.12, no.23, pp:10143, December 2020. https://doi.org/10.3390/su122310143

[7]. Mhlanga D., "The Role of Artificial Intelligence and Machine Learning Amid the COVID-19 Pandemic: What Lessons Are We Learning on 4IR and the Sustainable Development Goals," International Journal of Environmental Research and Public Health, vol.19, no.3, pp:1879, February 2022. https://doi.org/10.3390/ijerph19031879

[8]. Ramya G, Srinivasagan KG. Integrating Cybersecurity Threats into Smart Manufacturing: Best Practices and Frameworks. InArtificial Intelligence Solutions for Cyber-Physical Systems (pp. 120-138). Auerbach Publications.

[9]. Wu Y., "Cloud-Edge Orchestration for the Internet of Things: Architecture and AI-Powered Data Processing," IEEE Internet of Things Journal, vol.8, no.16, pp:12792 - 12805, August 2021. https://doi.org/10.1109/JIOT.2020.3014845

[10]. Akter S., Hossain A., Sajib S., Sultana S., Rahman M., et al., "A framework for AI-powered service innovation capability: Review and agenda for future research," Technovation, vol.125, pp:102768, July 2023. https://doi.org/10.1016/j.technovation.2023.102768

[11]. Ahsan M. and Siddique Z., "Machine learning-based heart disease diagnosis: A systematic literature review," Artificial Intelligence in Medicine, vol.128, pp: 102289, June 2022. https://doi.org/10.1016/j.artmed.2022.102289

[12]. Natarajan G, Balasubramanian S, Elango E, Gnanasekaran R. Leveraging artificial intelligence and machine learning for advanced threat detection in smart manufacturing. InArtificial Intelligence Solutions for Cyber-Physical Systems (pp. 101-119). Auerbach Publications.

[13]. Varoquaux G. and Cheplygina V., "Machine learning for medical imaging: methodological failures and recommendations for the future," npj Digital Medicine, vol.5, no.48, pp:1-8, April 2022. https://doi.org/10.1038/s41746-022-00592-y

[14]. Mijwil M. M., Aljanabi M., and ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime," Iraqi Journal For Computer Science and Mathematics, vol.4, no.1, pp:65-70, January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.0019

[15]. Trakadas P, Simoens P, Gkonis P, Sarakis L, Angelopoulos A, Ramallo-González AP, Skarmeta A, Trochoutsos C, Calvo D, Pariente T, Chintamani K. An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. Sensors. 2020 Sep 24;20(19):5480.

[16]. Mohammed A, Kumar MA, Raj P, Sangeetha M. Fortifying Smart Manufacturing against Cyber Threats: A Comprehensive Guide to Cybersecurity Integration, Best Practices, and Frameworks. InArtificial Intelligence Solutions for Cyber-Physical Systems (pp. 180-205). Auerbach Publications.

[17]. Mijwil M. M., Aljanabi M., and Ali A. H., "ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information," Mesopotamian journal of cybersecurity, vol.2023, pp:18-21, February 2023. https://doi.org/10.58496/MJCS/2023/004

[18]. Nwankwo CO, Chikwendu OC, Igbokwe NC. Enhancing Smart Manufacturing Supply Chains through Cybersecurity Measures. International Journal of Engineering Inventions. 2024 Dec 4; 13(12):1-6.

[19]. Mijwil M. M., Filali Y., Aljanabi M., Bounabi M., Al-Shahwani H., "The Purpose of Cybersecurity in the Digital Transformation of Public Services and Protecting the Digital Environment," Mesopotamian journal of cybersecurity, vol.2023, pp:1-6, January 2023. https://doi.org/10.58496/MJCS/2023/001

[20]. Mijwil M. M., Hiran K. K., Doshi R., Dadhich M., Al-Mistarehi AH , and Bala I., "ChatGPT and the Future of Academic Integrity in the Artificial Intelligence Era: A New Frontier," Al-Salam Journal for Engineering and Technology, vol. 2, no. 2, pp116-127, April 2023. https://doi.org/10.55145/ajest.2023.02.02.01569

[21]. Haque M. U., Dharmadasa I., Sworna Z. T., Rajapakse R. N., and Ahmad H., "I think this is the most disruptive technology": Exploring Sentiments of ChatGPT Early Adopters using Twitter Data," Arxiv, pp:1-12, December 2022. https://doi.org/10.48550/arXiv.2212.05856

[22]. Rudolph J., Tan S., and Tan S., "ChatGPT: Bullshit spewer or the end of traditional assessments in higher education?," Journal of Applied Learning and Teaching, vol. 6, no.1, pp:1-22, January 2023. https://doi.org/10.37074/jalt.2023.6.1.9

[23]. Shackelford SJ. Smart factories, dumb policy? Managing cybersecurity and data privacy risks in the industrial internet of things. Minn. JL Sci. & Tech... 2019; 21:1.

[24]. Mullet V, Sondi P, Ramat E. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access. 2021 Feb 3; 9:23235-63.

[25]. X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, "Designing blockchain-based applications a case study for imported product traceability," Future Gener. Comput. Syst., vol. 92, pp. 399–406, Mar. 2019

[26]. M. Westerkamp, F. Victor, and A. Küpper, "Tracing manufacturing processes using blockchain-based token compositions," Digit. Commun. Newt. vol. 6, no. 2, pp. 167–176, 2019.

[27]. S. Krima, T. Hedberg, and A. B. Feeney. Securing the Digital Threat for Smart Manufacturing: A Reference Model for BlockchainBased Product Data Traceability. Accessed: Jun. 21, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs

[28]. F. Benhamouda, H. Shai, and T. Halevi, "Supporting private data on hyperledger fabric with secure multiparty computation," IBM J. Res. Develop., vol. 63, p. 6, Mar. 2019.

[29]. P. Frey et al., "Blockchain for forming technology–tamper-proof exchange of production data," in Proc. 38th Int. Deep Draw. Res Group Annu. Conf., Enschede, Netherlands, Jun. 2019, p. 6.

[30]. D. Miller, "Blockchain and the Internet of Things in the industrial sector," IT Prof., vol. 20, no. 3, pp. 15–18, May/Jun. 2018.

[31]. K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in Proc. 50th Hawaii Int. Conf. Syst. Sci., Honolulu, HI, USA, Jan. 2017, pp. 1–10.

[32]. Q. Zhu and M. Kouhizadeh, "Blockchain technology, supply chain information, and strategic product deletion management," IEEE Eng. Manag. Rev., vol. 47, no. 1, pp. 36–44, Mar. 2019.

[33]. X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[34]. Nasir S, Zainab H, Hussain HK. Artificial-Intelligence Aerodynamics for Efficient Energy Systems: The Focus on Wind Turbines. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(5):648-59.

[35]. Raza A, Farhan S, Nasir S, Salamat S. Applicability of 3D printed fighter aircraft model for subsonic wind tunnel. In2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST) 2021 Jan 12 (pp. 730-735). IEEE.

[36]. Nasir S, Javaid MT, Shahid MU, Raza A, Siddiqui W, Salamat S. Applicability of Vortex Lattice Method and its Comparison with High Fidelity Tools. Pakistan Journal of Engineering and Technology. 2021 Mar 29;4(1):207-11.

[37]. Doshi R., Hiran K. K., Mijwil M. M., and Anand D., "To That of Artificial Intelligence, Passing Through Business Intelligence," In Handbook of Research on AI and Knowledge Engineering for Real-Time Business Intelligence, pp:1-16, 2023. https://doi.org/10.4018/978-1-6684-6519-6.ch001.

[38]. Lee J, Singh J, Azamfar M, Pandhare V. Industrial AI and predictive analytics for smart manufacturing systems. InSmart manufacturing 2020 Jan 1 (pp. 213-244). Elsevier.

[39]. Vijayakumari R, Chintalapati PV, Baskar K, Ateeq K. Enhancing Resilience in the Integration of Cybersecurity for Smart Manufacturing. InArtificial Intelligence Solutions for Cyber-Physical Systems (pp. 92-100). Auerbach Publications.

[40]. Al-mashhadani M. I., Hussein K. M., Khudir E. T., and ilyas M., "Sentiment Analysis using Optimized Feature Sets in Different Facebook/Twitter Dataset Domains using Big Data," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 1, pp: 64– 70, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.007

[41]. Azeem M., Abualsoud B. M., and Priyadarshana D., "Mobile Big Data Analytics Using Deep Learning and Apache Spark," Mesopotamian Journal of Big Data, vol.2023, pp:18–30, February 2023. https://doi.org/10.58496/MJBD/2023/003

[42]. Korkmaz A., Aktürk C., and Talan T., "Analyzing the User's Sentiments of ChatGPT Using Twitter Data," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 2, pp: 202–214, May 2023. https://doi.org/10.52866/ijcsm.2023.02.02.018

[43]. Chen L., Zhang X., Chen A., Yao S., Hu X., and Zhou Z., "Targeted design of advanced electrocatalysts by machine learning," Chinese Journal of Catalysis, vol.43, no.1, pp:11-32, January 2022. https://doi.org/10.1016/S1872-2067(21)63852-4

[44]. Mijwil M. M., "Deep Convolutional Neural Network Architecture to Detection COVID-19 from Chest X-ray Images," Iraqi Journal of Science, vol.64, no.5, pp: 2561-2574, May 2023. https://doi.org/10.24996/ijs.2023.64.5.38

[45]. Fei S., Hassan M. A., Xiao Y., Su X., Chen Z., et al., "UAV-based multi-sensor data fusion and machine learning algorithm for yield prediction in wheat," Precision Agriculture, vol.24, pp:187–212, August 2022. https://doi.org/10.1007/s11119-022-09938-8

[46]. Mijwil M. M., Doshi R., Hiran K. K., Unogwu O. J., and Bala I., "MobileNetV1-Based Deep Learning Model for Accurate Brain Tumor Classification," Mesopotamian Journal of Computer Science, vol.2023, pp:32-41, March 2023. https://doi.org/10.58496/MJCSC/2023/005

[47]. Vaishya R., Javaid M., Khan I. H., and Haleem A., "Artificial Intelligence (AI) applications for COVID-19 pandemic," Diabetes & Metabolic Syndrome: Clinical Research & Reviews, vol.14, no.4, pp: 337-339, August 2020. https://doi.org/10.1016/j.dsx.2020.04.012

[48]. Sivarajah U., Kamal M. M., Irani Z., and Weerakkody V., "Critical analysis of Big Data challenges and analytical methods," Journal of Business Research, vol.70, pp: 263-286, January 2017.

[49]. Oztemel E. and Gursev S., "Literature review of Industry 4.0 and related technologies," Journal of Intelligent Manufacturing, vol.31, pp:127–182, July 2018. https://doi.org/10.1007/s10845-018-1433-8

[50]. Mijwil M. M., Hiran K. K., Doshi R., and Unogwu O. J., "Advancing Construction with IoT and RFID Technology in Civil Engineering: A Technology Review," Al-Salam Journal for Engineering and Technology, vol. 02, no. 02, pp:54-62, March 2023. https://doi.org/10.55145/ajest.2023.02.02.007

[51]. Fanoro M., Božanić M., and Sinha S., "A Review of 4IR/5IR Enabling Technologies and Their Linkage to Manufacturing Supply Chain," Technologies, vol.09, no.04, pp:1-33, October 2021. https://doi.org/10.3390/technologies9040077

[52]. David L. O., Nwulu N. I., Aigbavboa C. O., and Adepoju O. O., "Integrating fourth industrial revolution (4IR) technologies into the water, energy & food nexus for sustainable security: A bibliometric analysis," Journal of Cleaner Production, vol.363, pp:132522, August 2022. https://doi.org/10.1016/j.jclepro.2022.132522

[53]. Hadjadj A. and Halimi K., "COVID-19 Patients' Health Monitoring System using Fuzzy Ontology and Internet of Things," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp:191–203, January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.0016

[54]. Nyagadza B., Pashapa R., Chare A., Mazuruse G., and Hove P. K., "Digital technologies, Fourth Industrial Revolution (4IR) & Global Value Chains (GVCs) nexus with emerging economies' future industrial innovation dynamics," Cogent Economics & Finance, vol.10, no.1, pp:1, January 2022. https://doi.org/10.1080/23322039.2021.2014654

[55]. P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, Jan. 2018.

[56]. E. H. Hwang, P. V. Singh, and L. Argote, "Knowledge sharing in online communities: Learning to cross geographic and hierarchical boundaries," Org. Sci., vol. 26, no. 6, pp. 1593–1611, 2015.

[57]. Z. C. Kennedy et al., "Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology," J. Mater. Chem. C, vol. 5, pp. 9570–9578, Aug. 2017.

[58]. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," IEEE Access, vol. 5, pp. 17465–17477, 2017.

[59]. N. Alzahrani and N. Bulusu, "A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol," Concurrency Comput. Pract. Exp., vol. 32, no. 12, p. e5232, 2020.

[60]. Z. Liu and Z. Li, "A blockchain-based framework of cross-border e-commerce supply chain," Int. J. Inf. Manage., vol. 52, Jun. 2020, Art. No. 102059.

[61]. J. Ma, S.-Y. Lin, X. Chen, H. M. Sun, Y.-C. Chen, and H. Wang, "A blockchain-based application system for product anti-counterfeiting," IEEE Access, vol. 8, pp. 77642–77652, 2020.