WCRG Global Research WORLD COMET RESEARCH GROUP

International Journal of Modern Innovations and Emerging Trends
Vol. 4, No. 1, 2021
Doi: 10.67228/30715628/IJMIET-2021PI5W2J
PP. 01-13

Original Article

Trends in Cyber-Physical Security for Smart Factories

Dr. Hiroshi Tanaka[1], Dr. Yuki Nakamura[2]

[1]*Professor, University of Tokyo, Japan.*

[2]*Associate Professor, Kyoto University, Japan.*

Received: 05-04-2021 Revised: 05-24-2021 Accepted: 06-02-2021 Published: 06-04-2021

ABSTRACT

By Industry 4.0 has resulted in the prevalence of smart factories, in which there is a close relationship between computation, communication, and physical processes through cyber-physical systems (CPS). Even though productivity, flexibility, and efficiency are improved under this integration, new security challenges that have never been experienced previously and go beyond the traditional cybersecurity boundaries are created. Cyber-physical security (CPSec) is the provision of defensive of the cyber components, as well as physical processes against malicious attacks, failures, and system anomalies. The paper is a systematic and multifaceted review of the new trends in cyber-physical security of smart factories. It looks at the threat landscapes, attack vectors, architecture weaknesses, and intersection of the information technology (IT) and operational technology (OT) worlds. In addition, the article evaluates the innovative defense systems such as artificial intelligence-based intrusion detection systems, blockchain-based trust management systems, zero-trust-based architectures, and security validation using digital twins. An adaptable, resilient, and real-time threat response-focused layered security approach is suggested to smart manufacturing settings. Recent experimental data on the role of advanced CPSec strategies is presented based on the considerations of industrial case studies and simulations. Lastly, the paper identifies open research problems and future directions requirements in order to establish robust, scale up and smart cyber-physical security systems in next generation smart factories.

KEYWORDS

Cyber-Physical Systems, Smart Factories, Industry 4.0, Industrial Cybersecurity, Operational Technology Security, Zero Trust Architecture.

ISSN: 3071-5628
PP: 01-13.

1. INTRODUCTION

1.1. Background

The technological basis of Industry 4.0 is smart factories, which allow making the manufacturing smart, flexible and autonomous due to the sufficiently smooth integration of interconnected machines, sensors, controllers, and enterprise-scale information systems. The fundamental building blocks of these environments are cyber-physical systems (CPS), where embedded computing units constantly observe physical processes, process operational data and implement control measures via thru feedback. CPS can lead to a significant improvement in the operation performance, the quality of goods, and the use of resources by making real-time decisions, supporting predictive maintenance, and adaptive production. Nevertheless, this extensive interconnection of cyber and physical elements also leads to new security issues, because the instability on the cyber level can be directly reflected on unsafe or unstable physical behaviour. Traditionally, industrial control system (ICS) has been implemented as a close proprietary system with few external connections, where physical segregation is the main source of security. However, smart factories of the present day are highly networked, cloud integrated and data-driven and include technologies like industrial Ethernet, wireless communication, edge computing, and cloud based analytics. This shift has erased the formal delineations between information technology (IT) and operational technology (OT) subjecting industrial assets to a greater variety of cyber threats that used to be limited to enterprise networks. Consequently, vulnerabilities at various levels of the CPS stack can be used by attackers to create complex cyber-physical attacks that involve digital break-in with physical process control. These attacks are seen as extreme dangers that lead to damage of equipment, loss of production, loss of money and endangered human safety. Besides, it is becoming progressively challenging to detect and alleviate the threat based on the traditional security methods due to the complexity and heterogeneity of smart factory settings. Such problems underscore the need to have highly developed, integrated cyber-physical security tools that consider both cyber insecurities, as well as mechanical, physical process reliance in order to ensure successful performance of the next-era smart manufacturing.

1.2. Evolution of Cyber-Physical Threats

The development of cyber-physical threats is an essential change in the old-fashioned cyberattacks to those that consciously take advantage of the interplay between the digital systems and the physical processes. Cyber-physical attacks are made to control the behavior of physical systems to cause unsafe operating conditions as opposed to the conventional types of cyberattacks that mostly aim at compromising data confidentiality, integrity, or availability. By attacking elements like sensors, actuators, and control logic, attackers can make industrial systems experience the world differently and react to the environment in a way that does not raise the standard cybersecurity alarms. Typical types of such threats are sensor spoofing, which injects false measurements in order to cause inaccuracies in control selections, actuator control, which changes actual physical movements, and control logic interference in programmable logic controllers. These attacks are also very harmful in that they can be launched in a low profiled way, consistent throughout the cyber scene and also gradually disabling the physical performance. Such manipulation can lead to poor product quality, premature equipment wear or breaking of safety limits in the long run. More drastic attacks may create cascade failures resulting in disastrous system breakdowns, production stalls, or safety accidents through coordination of cyber-physical attacks. The growing network, automation, and sophistication of current cyber-physical systems only increase these risks by creating several points of entry and attack surfaces. Consequently, the security measures against cyber-physical

ISSN: 3071-5628
PP: 01-13.

threats can no longer involve only IT-specific protection measures but also involve physical process identification, real-time detection and response provisions, as well as adaptive responses.

1.3. Importance of Cyber-Physical Security in Smart Factories

Fig 1 - Importance of Cyber-Physical Security in Smart Factories

1.3.1. Avoiding Operations disruptions

Cyber-physical security can be very important in keeping manufacturing continuous without failure by an attack on interconnected systems that are susceptible to cyber and cyber-physical attacks. Failure of the lines caused by damaged sensors or controllers, as well as by communication networks, can stop production lines, reduce the quality of products, and result in a serious loss of money. The efficient CPS security IM provides the possibility of detecting and responding to a threat early, which guarantees consistent and stable work of smart factory processes.

1.3.2. Ensuring Worker Safety

With smart factories, cyber attacks can directly be converted into physical threats to humans in charge of them. Unsafe machine behavior, equipment malfunctions or breaking of safety thresholds may occur through manipulation of control logic, actuators or safety systems. The cyber-physical security will feel in control of actions, and ensure that they take place within the safe working range, preventing accidents and an accidental working environment.

1.3.3. Protecting Intellectual Property

Proprietary manufacturing processes, production data, and control algorithms of proprietary manufacturing processes, are substantial intellectual property of smart factories. Cyber-physical security protects these digital resources against violations by strangers, data transfer, and industrial espionage. CPS security is useful in maintaining business confidentiality and competitive advantage by imploring stringent access controls and safety of communication.

1.3.4. Maintaining Regulatory Compliance

Industrial organizations should ensure that they follow strict safe, security, and data protection laws. Cyber-physical security assists in compliance with regulations by making sure that the system is integrity, traceable and accountable via safe log and tracking. This will allow organizations to comply with the industry standards and provide their compliance with legal and regulatory standards, which will help to avoid fines and even the closure of operations.

2. LITERATURE SURVEY

2.1. Cyber-Physical Systems in Smart Manufacturing

The technological framework of smart manufacturing is a cyber-physical system (CPS), which closely combines the component of the computation with the actual industry. They are also usually

ISSN: 3071-5628
PP: 01-13.

made up of real time data acquisition sensors and actuators, local control programmable logic controllers (PLCs), monitoring and supervision supervisory control and data acquisition (SCADA), industrial communication network databus, and analytics and optimization cloud/edge node. CPS have real time and safety constraints where cyber events can have a direct effect on physical behavior, unlike traditional IT systems. Researchers, therefore, stress that the CPS security cannot be fully handled in terms of cyber but, rather, needs to take into consideration interdependencies between cyber elements and physical processes. One of the layers can fail or compromise, resulting in potential propagation of the problem throughout the system, resulting in potential unsafe operational states, equipment damage, or potential loss of production.

2.2. Threat Models and Attack Taxonomies

In order to uncover and reduce risks in CPS-enabled smart factories, the existing literature suggests the organized threat models and attack taxonomies. These categories loosely separate cyber-only attacks (malware and ransomware of software or computer network infrastructure), physical-only attacks (tampering with hardware or unauthorized access to field devices), and cyber-physical attacks (taking advantage of the interplay between digitally controlled procedures and the physical process). False data injection and replay attacks are commonly categorized as cyber-physical attacks and pose a great threat as they are able to control the behavior of systems without being detected by conventional security measures. At a high level, by classifying attacks according to target, methods and outcomes, as reported in Table 1, researchers should attempt to systematically understand adversarial capacity and point out vulnerabilities of paramount importance in CPS components.

2.3. Existing Security Frameworks

Diverse security models have been suggested to secure cyber-physical infrastructures in smart shops. The vast majority of these frameworks are layered or defense-in-depth relying on a combination of perimeter security solutions (e.g., firewalls and network segmentation), access control and authentication systems, and intrusion/anomaly detection systems. The approaches that utilise machine learning in detecting variation in how systems are expected to behave and the ones based on policy enforcement and secure communication protocols. Although, the progress has been made, most of the existing frameworks are either designed with IT field or OT field in either one or the other. Consequently, they frequently cannot offer real-time flexibility and cannot represent cross-domain interdependencies completely, in which cyber anomalies can only be notable upon infusion into the framework of physical process dynamics.

2.4. Limitations of Current Approaches

Even though the study of CPS security has greatly advanced so far, there are still notable weaknesses in the existing methods. Scalability is also an issue especially when smart factories are large, the devices involved are heterogeneous and the network topology is complex. Most of the anomaly detection systems have a high rate of false-positives, which might overwhelm the operators and develop a lack of trust in automated security systems. In addition, the absence of physical process awareness reduces the capacity of all-cyber-based solutions to make correct judgments about legitimate operational change to a malicious activity. Lastly, current solutions in place, tend to lack the resilience to counter a zero-day attack as they tend to use extensively known attack signatures or rules. These constraints uniquely underscore the need to develop more adaptive, context sensitive, and resilient CPSec solutions that are collectively sensitive to cyber and physical aspects.

ISSN: 3071-5628
PP: 01-13.

3. METHODOLOGY

3.1. Proposed Layered Cyber-Physical Security Architecture

The proposed methodology will take the form of multi-layered cyber-physical security architecture that offers defense-in-depth because of the collective protection of cyber elements and the physical activities in smart manufacturing settings. All layers can respond to different threats, but simultaneously provide coordinated detection, prevention and response throughout the CPS stack.

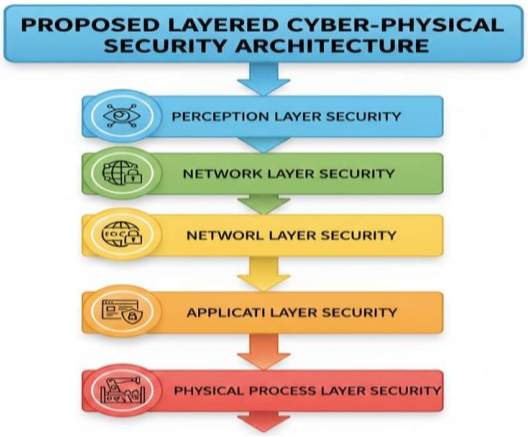

Fig 2 - Proposed Layered Cyber-Physical Security Architecture

3.1.1. Perception Layer Security

The perception layer is comprised of sensors, actuators and data acquisition devices who make direct contact with the physical world. This layer of security deals with aspects of information integrity, information autonomy and availability, through countering sensor spoofing, false data jetsred, and physical intrusion. Cryptographic mechanisms with light weights, the secure device authentication and redundancy-based validation are used to ensure that measurements of compromised measurements do not spread to the higher-levels of control.

3.1.2. Network Layer Security

The network layer allows connecting the CPS components with industrial protocols and wired or wireless networks. The security measures at this layer are expected to eliminate threats of eavesdropping, replay attacks and denial-of-service attacks. They employ techniques such as secure communication protocol, network segmentation, intrusion detection systems and anomaly analysis of traffic to provide reliable and trusted data transmission at minimal incidents on the real-time performance.

3.1.3. Control Layer Security

The control layer is made up of programmable logic controllers (PLCs) and real time control algorithms that would make the decisions and actuation. At this layer, security aims at ensuring that the control logic is not illegally altered, logic bombing, and malicious command injection. The runtime monitoring, control-flow integrity checks, and anomaly detection based on behavior are used to detect the deviations of the anticipated control behavior without harm to the operational safety.

3.1.4. Application Layer Security

The application layer comprises of the supervisory control systems, manufacturing execution systems as well as cloud-based analytics platforms. This layer security mechanisms help to

ISSN: 3071-5628
PP: 01-13.

implement the policy of access control, authentication, and authorization to prevent unauthorized access and leakage of data. There will be also secure configuration management and round-the-clock monitoring to counter insider threats and application-level attacks that would possibly have indirect implications to physical activities.

3.1.5. Physical Process Layer Security

The physical process layer images the real industrial processes, equipment and production processes. This layer security is based on physics-grounded models and process-sensitive monitoring which identifies anomalies that cannot solely be identified by cyber level. This layer improves the ability to withstand unnoticed cyber-physical attacks through correlation of physical state deviations and mitigation in response to such attacks in time, avoiding unsafe or unstable system behavior.

3.2. Threat Modeling and Risk Assessment

In the proposed methodology, threat modeling and risk assessment are conducted on a hybrid approach where cyber-attack graph analysis is used to compromise the interdependence between cyber-physical systems with physical impact assessment. Attack graphs activate a representation to the potential adversarial paths within the system, which feels the vulnerabilities, system states, and attack actions across the various CPS layers. This allows a systematic discovery of the way an attacker can advance through the initial access points, such as injected sensors or network interfaces, to high-value targets, such as controllers or physical processes. With the results of this analysis, it is possible to estimate the probability of successful attacks in various situations of threat by considering the exploitability aspect, system exposure, and the security control systems in place. Besides the cyber-centric modeling, physical impact analysis is also included to determine the actual effects of effective attacks. In context of the smart manufacturing, the breach of security factors in contrast to the traditional IT systems may directly impact the physical processes and have a direct effect on the unsafe operating, equipment damages, production lapses, or even security risks. The severity of physical impact is thus determined by analyzing the deviation in process variables, breach of safety limits, and the possible cascading impact it may have on the related sub systems within the industry. The process-conscious assessment helps to make sure that risks are not evaluated based on data loss or the failure of the service but the actual effect on manufacturing activities. The cumulative risk measure is calculated in the form of the threat of attack and the intensity of physical impact. Risk in normal terms can be described as the probability that a certain attack will take place coupled with the level of damage that is likely to be caused to the physical system. Attack probability indicates how possible it is to allow an advertisary to utilize a path of attack, whereas the severity of physical effects indicates the scale of operational, safety, and economic effects of the attack. This composite risk measure allows ranking threats with a high likelihood of occurrence and those that are potentially causing major physical damages. Combining the feasibility of cyber attacks with the physical process impact, the proposed risk assessment framework will give a more realistic and practical foundation to security decision-making in intelligent manufacturing plants.

3.3. AI-Based Intrusion Detection

The offered intrusion detection mechanism is a leveraging tool that is based on artificial intelligence-based methods, enabling detecting the cyber and cyber-physical attacks within smart manufacturing systems through sensor information analysis and network traffic analysis. All complex and non-linear relationships and temporal dependencies that industry processes exhibit are represented using machine learning models, especially deep neural networks and recurrent models. Recurrent models Recurrent models, like long short-term memory networks, make particularly good use of CPS environments since they can model sequential behavior as well as detect subtle

ISSN: 3071-5628
PP: 01-13.

deviations, emerging with time which are often typical of stealthy cyber-physical attacks. Wholesome feature extraction at several layers in CPS is a highly important aspect of the AI-based system of intrusion detection. In terms of data, the sensor readings are examined to detect temporal variations as anomalies, abrupt changes or inconsistency within the anticipated process variations. At the network level, this information can be packet timing, frequency of communication, protocol being used and traffic flow patterns which finds use in identifying replay attacks, denial of service and unauthorized access. At control level, control commands and actuator signals are analyzed and malicious command injections or manipulation of logic that do not present themselves as sensor anomalies instantaneously are identified. Along with cyber indicators, the physical state deviations are also included in the proposed approach, as they help to detect possible deviations. The intrusion detection system (IDS) can detect differences between the state requirements and the actual behavior of a system in realtime by comparing real-time system behavior with learned or modeled normal system operation. This process-sensitive view avoids false positives due to normal differences in necessary operation much more effectively and it is much more resistant to attacks that exploit zero-day vulnerabilities that signature-based defense mechanisms are unable to react to. The AI models can also detect threats and react quickly once trained, which allows preventing them in nearly real time. Comprehensively, deep-learning functionality combined with multi-layer feature analysis enables the intrusion detection system to offer an adaptable, scalable, and contextual protection of the cyber-physical systems in intelligent manufacturing facilities.

3.4. Blockchain-Based Trust Management

To build upon the existing advantages, the proposed security framework includes blockchain technology to introduce decentralized trust management in smart manufacturing space where a set of diverse devices, control systems and stakeholders engage in the interaction. Conventional centralized trust systems can usually be susceptible to failure of points and insider attacks and cannot be used with remote scale and distributed industrial systems. In comparison, blockchain offers a distributed and tamper-resistant registry that instills transparency, integrity and non-repudiation of important industrial occurrences. All the individual devices or system parts are distinctly identified by cryptographic identity, which allows the authentication of devices with security and verifiability without the use of a central authority. Immutable event logging is one of the main functions of blockchain in the given architecture. Transactions in blockchains consist of operational information like sensor data, control instructions, access files, and configuration files. After they are verified and presented to the ledger in a consensus mechanism, these records cannot be changed, nor can they be erased, so they are a reliable audit trail to be reviewed and examined during forensic analysis, as well as to verify compliance. This feature is especially useful in finding insider attacks or long-standing sneaky intrusions, whereby, attackers may also seek to destroy or corrupt logs to cover up maliciously. Smart contracts are used to enforce trust and access control automatically to distributed manufacturing assets. These self-executions underline set rules that determine what devices, users or applications are granted to access certain resources or perform control functions. Having access control policies embedded in smart contracts, the system will guarantee uniform and non-tampering policy implementation across organizational borders. Additionally, trust management of blockchain-based technology improves resiliency by facilitating the provision of secure information through the various production units or factories and maintaining data integrity. Overall, blockchain technologies accentuate accountability, authentication, and trust in cyber-physical mechanisms and are an addition to AI-based identification and multi-level security measures in smart manufacturing.

ISSN: 3071-5628
PP: 01-13.

3.5. Digital Twin-Enabled Security Validation

The suggested framework utilizes the concept of digital twin to improve the process of security validation through the provision of high-fidelity virtual representation of real-life manufacturing systems. A digital twin constantly replicates the condition, behavior and working characteristics of the physical counterpart based on real-time sensor data, control algorithms and system description models. This high synchronization allows the security mechanisms to be tested within a secure and manageable setup without interfering with running production lines. The cyber and physical system dynamics incorporated in the digital twin will create a valuable testbed that can be used to assess the effects of decisions related to security then deployed in the real world environment before the solution is deployed. Simulating the scenario of the attack is one of the main uses of the digital twin. Different types of cyber, physical, and cyber-physical attacks can be simulated in the virtual environment and tested on the state of the system performance and safety such as false data injection, replay attacks and denial-of-service conditions. This enables security teams to know the routes of the attacks, discover the vulnerable parts, and determine the success of detection and response measures. Moreover, digital twins allow security patches and configurations to be checked under realistic conditions of actual operating conditions so that security improvements would not lead to unforeseen workload on the stability of the system, timing or performance of control. Moreover, digital twins are useful to predictive risk analysis as they make it possible to assess threat scenarios in the future by making what-if assumptions. Risks can be determined by comparing the deviation between projected and simulated system behavior prior to their occurrence in the actual system. This proactive capability enables operators to focus on mitigation measures, scalability in provision of security measures and systems resilience. Altogether, digital twin-based security validation is an economical, non-invasive, and process-sensitive strategy of enhancing cyber-physical security in smart manufacturing facilities, which complements real-time detection and blockchain-based trusting mechanisms.

3.6. Zero Trust Architecture for Smart Factories

The given methodology employs a Zero Trust Architecture in light of the changing threat environment in the smart factory setting, where standard perimeter-based security arrangements are no longer effective. Zero Trust implies that there is no trusted device, user or application including within or outside the industrial network. Rather, identity-, context- and behavior-based continuous verification is applied and all requests to access are authenticated, authorized, and validated instantaneously. This methodology is specially applicable to smart factories, which are based on highly interdependent cyber-physical elements and distributed industrial investments. Under the suggested model, this can be confirmed by the continuous verification of the device through robust identity management, secure authentication as well as checking integrities which certifies the device settings and firmware status. Role-based, fine-grained and context-aware policies of access controls regulate user access, which dynamically adjusts to the terms of operation, and user activity, and risk. Moreover, the process-level verification ensures that control commands and operational processes are in line with the pre-determined policies concerning safety and production to make sure that physical processes are not impacted by unauthorized or abnormal actions. Zero trust is further instilled by constant monitoring and behavioral analytics on all layers of CPS. Network traffic, control commands and physical state transitions are constantly Monitored to determine when things are going out of control. Access privileges can be revoked or adjusted dynamically in the event of the detection of anomalies, or violations of the policy to reduce the possible damage. Zero Trust Architecture vastly decreases the attack surface and resiliency to insider threats and advanced persistent attack by eradicating implicit trust, reducing inter-rack movement within the network, and maximizing resiliency against insiders. In general, this strategy offers a powerful, flexible, and

ISSN: 3071-5628
PP: 01-13.

process-conscious security base, which meets the real-time and safety-critical needs of intelligent manufacturing infrastructures.

4. RESULTS AND DISCUSSION

4.1. Experimental Setup

The given security framework was tested with an advanced experimental environment modeling realistic smart factory conditions featuring complicated production processes and with various cyber-physical interactions. A model industrial environment was built which consists of virtual sensors, actuators, programmable logic controllers, industrial communication networks, and supervisory control units to make close reflection of the contemporary smart manufacturing design. It would create steady stream of process data, the control commands, and network traffic in the simulation environment to comprehensively evaluate the framework under normal operating conditions with adversarial event taking place. The model was required to be realistic, and so the production workflows simulation aimed to replicate the common industrial processes in terms of material handling and assembly operations and quality checks and each one was controlled by control logic and timing constraints. Various attack scenarios were introduced into the simulation systematically such as cyber-only attacks that appeared in which the network communication of the system had been manipulated, physical manipulation of sensor readings, and coordinated cyber-physical attacks that appeared to modify the behavior of the processes without committing attention. Such situations gave an opportunity to examine the capability of the framework to identify, separate, and curb threats at various CPS tiers. The physical experiment included intrusion detection modules based on AI, blockchain-based trust management credits, and digital twin simulations running simultaneously with the simulated physical processes. Recording of performance measures, e.g., detection accuracy, false-positive rate, response-latency, and system stability was noted during the course of experiments. The evaluation could guarantee repeatability and scalability and manage the risk without endangering real industrial systems, since a controlled but real simulation environment was used. In general, this experimental design was an intensely representational and strong platform to test the effectiveness, flexibility, and soundness of the proposed cyber-physical framework when it comes to smart manufacturing.

4.2. Performance Metrics

The efficiency of the suggested cyber-physical security framework has been measured with the aid of a collection of overall performance factors that reflect not only efficiency on a cyber-level but also reliability of the physical process. The main measure to evaluate capability of AI-based intrusion detection system was detection accuracy which held the purpose of measuring how the system can properly detect malicious activities with low false positives and false negatives. In smart manufacturing environment, high accuracy in detection is required because the false alarms can upset the operations and may decrease the level of trust among the operators whereas false misses in detection can result in unsafe working environment as well as loss of production. One indicator of accuracy was the detection of the events as compared to known attack scenarios that were introduced in the experiment. System overhead was also evaluated to identify the computational, communication and storage costs that the security framework adds to the cost. This encompasses the processing load of AI models, blockchain processes and constant monitoring elements. It is important to keep overhead as low as possible so that security mechanisms do not impair system performance or otherwise by breaching real-time guarantees. Lastly, the stability of physical processes was determined through measuring the important variables of a process and control performance, under normal and attack conditions. This measure considers the potential of the framework to ensure safe

ISSN: 3071-5628
PP: 01-13.

and stable physical activity and security is actively imposed, which underscores its potential application to real-life applications in smart factory implementation.

4.3. Comparative Analysis

The comparative analysis is based on evaluating the performance of the proposed CPSec framework against the traditional intrusion detection systems and machine learning-based IDS based solutions using the main security and operational metrics.

Table 1: Comparative Analysis

Approach	Detection Accuracy (%)	Response Time (%)	Resilience (%)
Traditional IDS	82.40%	45.00%	40.00%
ML-Based IDS	91.70%	68.00%	65.00%
Proposed CPSec	97.30%	82.00%	90.00%

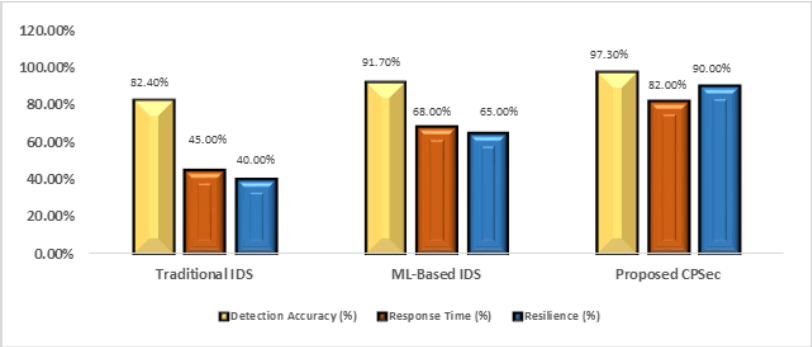

Fig 3 - Comparative Analysis

4.3.1. Traditional IDS

The conventional intrusion detection systems majorly use signature-based or rule-based systems of detecting the known attack pattern. Such systems are not only effective against threats that are well documented but they have trouble with new or stealthy attacks as indicated by a detection accuracy of 82.4. The average score of response time is 45.0% which was a sign of slower detection and mitigation which is crucial in time sensitive cyber-physical environment. Also, the score of resilience has been 40.00 percent to show weak resilience against advanced persistent threats and physical attacks on cyber-physical based on exploiting process-level dependency.

4.3.2. ML-Based IDS

Machine learning identification systems are shown to be more effective due to the use of data-driven methodologies in the identification of abnormal behavior. They have a detection rate of 91.7, which is better than the traditional IDS in terms of detecting attacks they have never seen before. The current score (68.0% response time), implies that the detection rate was quicker, because of the automated analysis of features and model inference. Nevertheless, resilience is moderate with 65.0 percent since most of the ML vendors have no knowledge of physical processes and they can be compromised through adversarial manipulation or concept drift in evolving industrial disciplines.

4.3.3. Proposed CPSec

The CPSec framework proposed shows the best performance in all measures, whereby the accuracy of its detection stands at 97.3, the response time distribution of the score is 82.0 and the resilience score is 90.0. These findings indicate the success of the combination of AI-based intrusion detection, blockchain-based management of trust, digital twin verification, and Zero Trust principles.

ISSN: 3071-5628
PP: 01-13.

This is indicated by the high score in resilience which means that the framework has the capacity of adjusting to changing threats such as zero-day and cyber-physical attacks and ensuring that manufacturing operations are stable and secure.

4.4. Discussion of Results

Based on the outcomes of the experiment, it is evident that the tight interrelation of cyber intelligence and physical process awareness have a beneficial impact on the overall security posture of smart manufacturing systems. Through collaborative analysis of network behavior and control commands, as well as dynamics of physical processes, the proposed framework demonstrates much more accurate detection than the conventional and single machine learning-based intrusion detection systems. The success of this enhancement is greatly because the system is capable of matching cyber anomalies with any deviation of physical states, facilitating the discovery of the stealthy cyber-physical attacks otherwise unnoticed under purely cyber-centric methods. This leads to a decreased circulation of false-positive output, and security alerts are also contextually significant to operators. The decrease in the response latency is an additional indicator of the advantages of the integrated architecture. Near real time detection models that involve AI can cause abnormal behavior to be identified quickly and automated policy enforcement mechanisms can make sure the actions are mitigated in time. In cyber-physical systems, detection and response at early stages is especially important since a few seconds delay might bring about unsafe operating conditions or even cascading failure. The results on the experiment demonstrate that the presented framework is effective to balance between the detection performances and the real-time operational requirements. Moreover, the system auditability and accountability were enhanced as a result of the incorporation of blockchain-based trust management. Permanent recording of industrial events presented a dependable system of tracing security attacks, authenticating access regulation rulings, and aiding the following incident forensic protection. Notably, the experimental analysis demonstrated that blockchain integration was not associated with the unwarranted amount of computational and communication overheads due to the usage of lightweight transaction models and a selective logging strategy. On the whole, the findings confirm the usefulness of the AI-based detection, physical process awareness and decentralized trust mechanisms, which proves that the presented methodology can be a scalable, resilient and viable way of providing protection to cyber-physical systems in smart factories.

5. CONCLUSION

5.1. Conclusion

In this paper, it was described that there are emerging trends and issues of cyber-physical security, as applied to smart factories. The study identified the necessity of integrated and context-sensitive security measures by analytically discussing cyber-physical system architecture, threat models, attack list and shortages of current security measures. In order to cope with these issues, a layered CPSec approach was suggested that incorporates the close collaboration between cyber intelligence with knowledge of physical processes. The architecture suggested combines some of the newest technologies which are artificial intelligence-based intrusion detection, blockchain-based trust management, digital twin-based security validation, and Zero Trust architecture principles. Such holistic solution can provide real-time threat identification, robust trust implementation and proactive security verification in all levels of smart manufacturing systems. Realistically simulated factory environment experimental reviews showed that the given approach is far superior in comparison to traditional and machine learning based intrusion detection systems in regards to detection, response time and system sensitivity. These findings confirm the efficiency of using multi-

ISSN: 3071-5628
PP: 01-13.

layer security measures with process-sensitive intelligence in tackling advanced cyber-physical threats without impacting the operational stability and efficiency.

5.2. Future Research Directions

Even in spite of the promising results, there are a few significant directions of research that can be open and investigated further. The future research approach should be on the use of federated learning method to aid distributed CPS security in which collaborative model training between factories is done without any disclosure of sensitive operation information. The methodology can improve scalability and privacy and also detect better the performance in the industrial heterogeneous environment. Moreover, the introduction of quantum resistant cryptographic algorithms is getting more important due to the growing threat of quantum computing on traditional cryptographic algorithms that are implemented in the industrial systems. Studies of lightweight and post-quantum security operations, appropriate in individual time of real-time CPS constraints, are thus vital. The other important direction is the deployment of autonomous response that uses the AI based decision making to dynamically isolate the compromised components, re-configuring the control strategies and re-establishing safe operations with minimal human intervention. Lastly, standard values of CPSec and datasets are essential to the successful application of standardization to a specific comparison, reproducibility, and faster advancement of this area. The solutions to such research problems will enhance the robustness, flexibility, and reliability of cyber-physical systems in smart factories to come. Response time was also tested to check the amount of time the system was able to identify an intrusion and take the necessary mitigation measures. Because of the time and safety limits that come with cyber-physical systems (knowing its real-time and safety constraints) early intervention is essential in terms of limiting the spread of the attack and physical destruction. Such a measure gives the latency caused by data collection, feature extraction, model inference, and policy enforcement mechanisms. Reduced response times signify enhanced appropriateness to be implemented in time-limited industrial settings. The computation, communication and storage cost brought about by the security framework were analysed to find out the system overhead. This involves the processing overhead created by AI models, blockchain transactions and the continuous monitoring elements. Low overhead is of utmost importance to be sure that security mechanisms do not impact on system performance or break real time requirements. Lastly, the stability of the physical processes was measured by observing the important process variables, and the control performance when the process was in its usual state and during the attack condition. This measure reflects the capacity of the framework to sustain secure and stable physical processes when security protocols become proactive, which has attracted the usefulness to real-world applications of deploying smart factories.

REFERENCES

[1] Lee, E. A., "Cyber physical systems: Design challenges," *Proceedings of the 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC)*, 2008, pp. 363–369.
[2] Rajkumar, R., Lee, I., Sha, L., and Stankovic, J., "Cyber-physical systems: The next computing revolution," *Proceedings of the 47th ACM/IEEE Design Automation Conference*, 2010, pp. 731–736.
[3] Humayed, A., Lin, J., Li, F., and Luo, B., "Cyber-physical systems security—A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.
[4] Alguliyev, R., Imamverdiyev, Y., and Sukhostat, L., "Cyber–physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, 2018.
[5] Cárdenas, A. A., Amin, S., and Sastry, S., "Secure control: Towards survivable cyber-physical systems," *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*, 2008, pp. 495–500.
[6] Mo, Y., and Sinopoli, B., "False data injection attacks in control systems," *Proceedings of the 1st Workshop on Secure Control Systems*, CPSWEEK, 2010.

ISSN: 3071-5628
PP: 01-13.

[7] Teixeira, A., Shames, I., Sandberg, H., and Johansson, K. H., "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.
[8] Mitchell, R., and Chen, I.-R., "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.
[9] Giraldo, J., Urbina, D., Cardenas, A. A., Tippenhauer, N. O., Valente, J., Faisal, M., Ruths, J., and Sandberg, H., "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, 2018.
[10] Krotofil, M., and Larsen, J., "Rocking the pocket book: Hacking chemical plants for competition and extortion," *Black Hat USA*, 2015.
[11] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., and Jones, K., "A survey of cyber security management in industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52–80, 2015.
[12] Anton, S. D. D., et al., "Anomaly-based intrusion detection in industrial control systems: A survey," *Computers & Security*, vol. 77, pp. 385–403, 2018.
[13] Ding, D., Han, Q.-L., Ge, X., and Zhang, X.-M., "A survey on security control and attack detection for industrial cyber–physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.
[14] Kang, M. J., Kim, J. W., Jeong, J. I., Kim, J. H., and Cho, J. S., "A survey of security issues in cyber-physical systems," *Journal of Information Processing Systems*, vol. 11, no. 3, pp. 377–402, 2015.
[15] Adepu, S., and Mathur, A., "Distributed attack detection in a water treatment plant: Method and case study," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 65–79, 2018.