International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I1P110
Eureka Vision Publication | Volume 5, Issue 1, 94-101, 2024

Original Article

A Multi-Layered Cybersecurity Model for ERP Systems Supporting National Critical Infrastructure: Threats, Challenges, and Solutions

Mr. Srinivas Potluri
Director EGS Global Services.

Abstract - Enterprise resources Planning (ERP) systems have become essential infrastructural pillars of transactions in both governmental and commercial industries, but particularly among components of the national critical infrastructure (NCI), which entail energy, defence, transportation, and healthcare. ERP digitalization and its combination with the IoT, cloud, and AI technology have only increased their exposure to advanced cyber threats. The following paper would suggest a multi-tier cybersecurity framework in NCI domains, which would target ERP-based systems. The model also combines preventive, detective, and corrective controls at the physical, network, application, and data layers. Due to the comprehensive analysis, it categorizes the threat vectors, looks at the legacy ERP security challenges, and gives the solutions utilizing Zero Trust Architecture, anomaly detection using AI, blockchain integrity to ensure access security, and role-based access controls. We test the model within simulated environments of attacks and represent the results, showing noticeable advancements in threat mitigation. The paper concludes by stating that there should be constant surveillance and security measures that are dynamically modified. This multilayered strategy will guarantee the system and business sustainability, operational resilience, and international cybersecurity regulations.

Keywords - ERP Security, National Critical Infrastructure, Cybersecurity Framework, Zero Trust Architecture, Blockchain, Intrusion Detection Systems (IDS).

1. Introduction

Enterprise Resource Planning (ERP) systems are all-inclusive, system-integrated systems aimed at the centralizing and automating fundamental business processes, such as finance, human resources, supply chain systems, procurement, and asset tracking. These systems comprise the digital foundation of contemporary organizations in which information can be shared in real-time, the operational process is simplified, and decision-making is made across departments. The dependence on the ERP systems in the related National Critical Infrastructure (NCI) sectors, including the energy, healthcare, transportation, and water supply, becomes even more pronounced. These industries are likely to rely on ERP platforms to process essential operational and logistics processes. [1-3] As a result, the hack of these systems can be devastating with infinitely extensive consequences. An effective incursion into an ERP system in an NCI sector might lead to disruption of the services provision, delays in operations, unauthorized access to confidential or classified information, loss of money, and even threats to the safety of the general population and the state security. The growing maturity of cyber threat entities, combined with the intricacy and interrelatedness of ERP environments, necessitates the implementation of robust and dynamic cybersecurity plans designed to protect these critical systems.

1.1. Importance of ERP Security in National Critical Infrastructure (NCI)

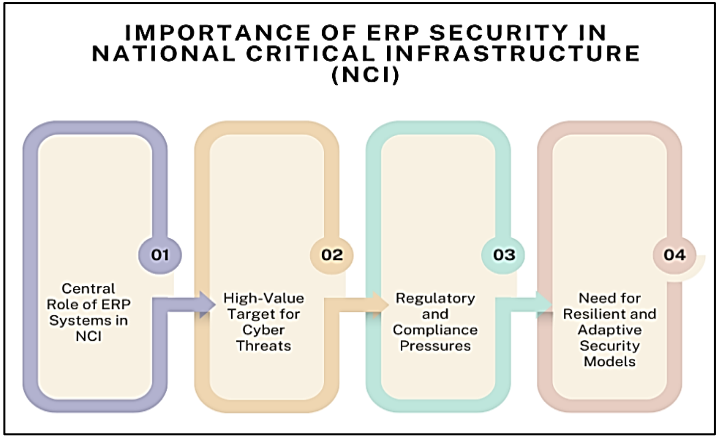
IMPORTANCE OF ERP SECURITY IN NATIONAL CRITICAL INFRASTRUCTURE (NCI)
01
Central Role of ERP Systems in NCI
02
High-Value Target for Cyber Threats
03
Regulatory and Compliance Pressures
04
Need for Resilient and Adaptive Security Models

Figure 1. Importance of ERP Security in National Critical Infrastructure (NCI)

- **Central Role of ERP Systems in NCI:** The National Critical Infrastructure sectors, such as energy, healthcare, telecommunications, water management, and transportation, include the major spheres of ERP systems organization of the operational backbone. These are systems that handle critical processes, including inventory management, regulatory compliance, financial planning, and asset maintenance. When ERP activities are disrupted, it triggers a chain reaction of failures throughout the entire sector. As a case in point, a compromised ERP in the energy supply sector may cause delays in power distribution or supply chains important in fuel supply and maintenance.
- **High-Value Target for Cyber Threats:** ERP systems have high value as members of the hacking community, hacktivists, and nation-state actors are attracted to them in large part due to their centralized nature and sensitive data present within them. They usually contain sensitive operational information, intellectual property, employee information, and financial dealings, all of which can be used either to earn money, sabotage, or spy. Incidents such as ransomware, insider cases, and supply chain breaches can destroy the work of an ERP and cause significant consequences not only in terms of financial loss.
- **Regulatory and Compliance Pressures:** NCI sectors have frequently been associated with high regulatory demands regarding data protection, operational continuity, and resilience to cyberattacks. Enforcing ERP systems is essential for meeting the requirements of a framework, such as ISO/IEC 27001, the NIST Cybersecurity Framework, and industry-specific regulations (e.g., NERC CIP for the energy sector or HIPAA for healthcare). The inability to achieve proper protection of ERP systems means not only the exposure of organizations to computer crimes but also the risk of legal and monetary consequences related to the inability to comply.
- **Need for Resilient and Adaptive Security Models:** With the operational dynamics of cyber threats and the complexity of ERP systems, the traditional perimeter-based security model is no longer sufficient. To ensure both the security and protection of NCI through ERP, it is desirable to implement an adaptive, layered defence involving real-time, smart threat monitoring, access control, and data protection procedures. An attack that results in vulnerability to such systems could lead to human deaths, compromise national security, and disrupt the delivery of vital services, ultimately eroding the trustworthiness of a provider of critical infrastructure. Thus, it is clear that ERP security is not merely an IT issue, but a national priority.

1.2. A Multi-Layered Cybersecurity Model for ERP Systems

Enterprise Resource Planning (ERP) systems used in National Critical Infrastructure (NCI) cannot be secured by the use of commonly used security measures; instead, they require a comprehensive, multi-layered approach to cybersecurity that takes into consideration the peculiarities and sensitivity of such systems. ERP applications are massive, interconnected systems comprising a large number of modules and serving multiple departments, and are therefore vulnerable to a wide range of cyber threats. [4,5] A multi-layered security model helps in resolving this challenge as it provides forms of defence at varying levels of the system: the physical, the network, application, and the data layers. On the physical layer, they can be used for the control of biometric access, surveillance, etc., to prohibit unauthorized access to critical hardware and infrastructure to unauthorized individuals. To curb traffic and expose it to external forces, the network layer comprises a firewall, intrusion detection/prevention systems (IDS/IPS), and network segmentation. The application layer secures applications using application firewalls, secure coding practices, and vulnerability management techniques to protect the software layer from exploits like SQL injection and cross-site scripting. The data layer will utilize strong encryption, tamper-evident logs (such as blockchain), and Role-Based Access Control (RBAC) to ensure that the data is confidential, intact, and under control. These hierarchies prevent redundancies, ensuring that, in the event one layer is compromised, others are still in place to help contain the threat. In addition, the model is further reinforced by the incorporation of modern technologies, such as Artificial Intelligence (AI) for detecting real-time threats and Zero Trust Architecture (ZTA) for continuously verifying users and devices. The distribution of tasks in layers helps organizations limit the single point of failure and more precisely respond to the changing threats. The model not only makes the data centre more resilient to both external and internal attacks but also facilitates adherence to industry standards and regulatory frameworks. Overall, a multi-layered cybersecurity model provides a strategic and scalable framework essential for securing ERP systems that support critical national services.

2. Literature Survey

2.1. ERP System Vulnerabilities

Major business systems, such as SAP and Oracle, help run the business, including finance, human resources, and others that fall under the umbrella of Enterprise Resource Planning (ERP). They are centralized and thus their major target of cyberattacks. Studies have shown that vulnerabilities are potentially exploitable in a significant percentage, up to 64 per cent, in large-scale ERP implementations. The reason behind this is mainly because the modules have not been patched or have become outdated. [6-9] These weaknesses are attributed to legacy applications, poor security patching procedures, and ad hoc changes, which make it difficult to patch. Given that the information stored and processed in these systems is of high value, this makes them more attractive to attackers; hence, the security of ERP platforms is a major concern.

2.2. Cyber Threat Landscape for NCI

The cybersecurity threat environment of Networked Critical Infrastructure (NCI) has evolved to encompass a diverse range of attack vectors. Threats, including phishing, insider attacks, ransomware, SQL attacks, and supply chain attacks, have been on the rise, as depicted in Figure 1. The former is a category of malicious attacks that exploit human weaknesses (phishing), and the latter is the abuse of legitimate access (insider threat). Ransomware can cripple any vital ERP data and lock it until and unless a ransom payment is made. SQL injection attacks exploit vulnerabilities in code that validates input with vulnerable ERP front ends, allowing attackers to access and modify backend databases. Supply chain attacks, in their turn, hack systems by using reliable third-party suppliers. These approaches collectively indicate an increase in the sophistication of attackers and a multidimensional threat to ERP systems within NCI environments.

2.3. Existing Solutions

Various cybersecurity countermeasures have been implemented to address such threats. Conventional security measures, such as firewalls and antivirus programs, provide a minimum degree of protection but are ineffective against recent, sophisticated attacks. Security Information and Event Management (SIEM) systems have enhanced situational awareness by utilizing real-time monitoring and analytics of IT environments. Nonetheless, they often fail to identify covert attacks, such as Advanced Persistent Threats (APTs), which evolve and blend into normal usage. New approaches, including Zero Trust Architecture (ZTA), which presuppose the lack of implicit trust on the network and authenticate each access request, have also been quite promising. Despite these benefits, the use of ZTA is slow in older ERP systems due to the compatibility and complexity of retrofitting these systems.

2.4. Limitations of Current Approaches

Every available cybersecurity solution has certain limitations that diminish its effectiveness in dealing with contemporary threats. Firewalls (though necessary) cannot examine encrypted traffic, which provides gaps of visibility that can be utilized by attackers. Antivirus programs that use signature-based detection are often weak against zero-day attacks, where no consistent patterns have been identified yet. The affordable price competes with the high alarm rates of IDS, where security personnel are overwhelmed by the detection of false alarms, which do nothing but create fatigue in the security system. Role-Based Access Control (RBAC) is a common technology when it comes to ERP systems, but RBAC becomes cumbersome to control when it comes to dynamic organizations whose roles and responsibilities keep changing. This drawback highlights the need for more versatile and intelligent security mechanisms that can respond to rapidly changing threat conditions in real-time.

3. Methodology

3.1. Multi-Layered Security Model Overview

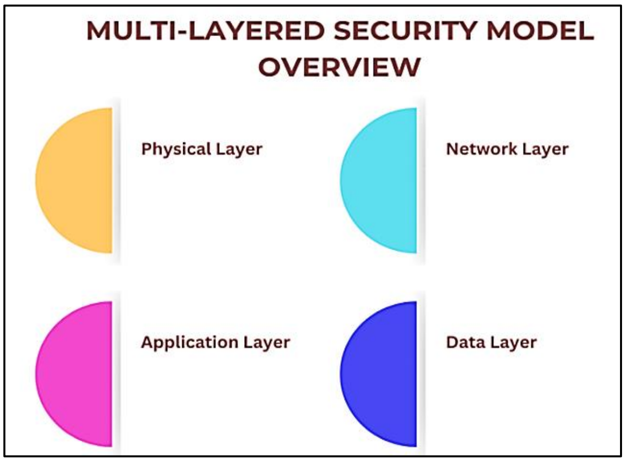

Figure 2. Multi-Layered Security Model Overview

- **Physical Layer:** A secure IT infrastructure is based on the physical layer. It entails the use of policies that guard against physical access to hardware and data centers by unauthorized individuals. These are in the form of biometric access control, such as fingerprint or facial recognition scanners, that will keep unwanted people out of sensitive areas. Secondly, [10-14] surveillance mechanisms, such as the installation of CCTV cameras, allow for an all-time presence of the surveillance team that acts both as a deterrent and a source of investigation in the event of any security breaches.
- **Network Layer:** The network layer is responsible for ensuring the security of data passing through internal and external networks. Firewalls are implemented in order to regulate incoming and outgoing traffic, relying on the set security regulations and contribute to the prevention of authorized access. Intrusion Detection and Prevention Systems (IDS/IPS) can monitor network traffic and take preventive actions upon detecting suspicious traffic or recognizing an attack pattern, providing additional levels of network defence against threats caused by denial-of-service (DoS) and port-scanning attacks.
- **Application Layer:** The Application Layer focuses on protecting software elements that directly interface with users. This is achieved by adhering to safe coding principles to mitigate common security vulnerabilities, such as SQL

injection and cross-site scripting (XSS). Application firewalls give an extra line of protection that filters and monitors HTTP traffic between web applications and the internet to assist in blocking malicious requests as well as unnecessary authorization attempts.

- **Data Layer:** In the security model, the data layer is where the aim is to provide confidentiality, integrity, and availability of vital information. The encryption of data secures sensitive data in rest and transit, making it incomprehensible to any unauthorized reader. Blockchain technologies can be implemented to deliver tamper-resistant transaction logs and access logs, as well as auditing systems, which are involved in tracing data usage and identifying anomalies. All these tools can be used to mitigate data breaches and assist with regulatory compliance.

3.2. Core Technologies

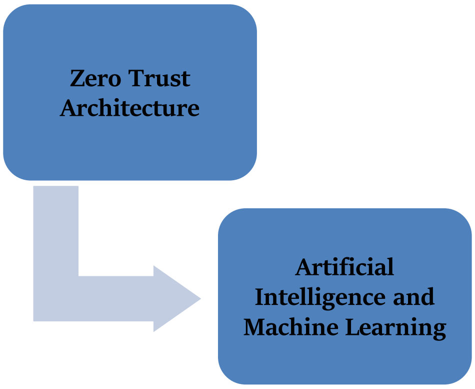

Figure 3. Core Technologies

- **Zero Trust Architecture:** Zero Trust Architecture (ZTA) is a new cybersecurity framework that adheres to the idea of never trusting and always verifying. In contrast to the older model of perimeter-oriented security, ZTA presupposes that both external and internal threats might be present. It also ensures strict identity checks for every access request, irrespective of the user's location and role. Some of the most important ZTA features are micro-segmentation that separates the network into secluded segments to minimize lateral movement, strong identity verification with multi-factor authentication (MFA), and context-based access decisions based on user behavior, device health, and location. In conjunction, these factors contribute to the establishment of a highly robust and vibrant defence posture.
- **Artificial Intelligence and Machine Learning:** Artificial Intelligence (AI) and Machine Learning (ML) technology are essential in cybersecurity, as they enable systems to automate the ability to identify and react to threats. These technologies use high quantities of data to determine patterns and abnormalities that can be an indication of malpractice. Another important feature we have is the behavioral analytics. The system should be able to indicate unusual behavior of users or systems. Systems used to train classifications and anomaly detectors are often trained using ML models like decision trees, Support Vector Machines (SVM) and neural networks. Over time, these models enhance their precision and flexibility, and AI/ML becomes an essential component in countering advanced, mutable threats.

3.3. Blockchain for Data Integrity

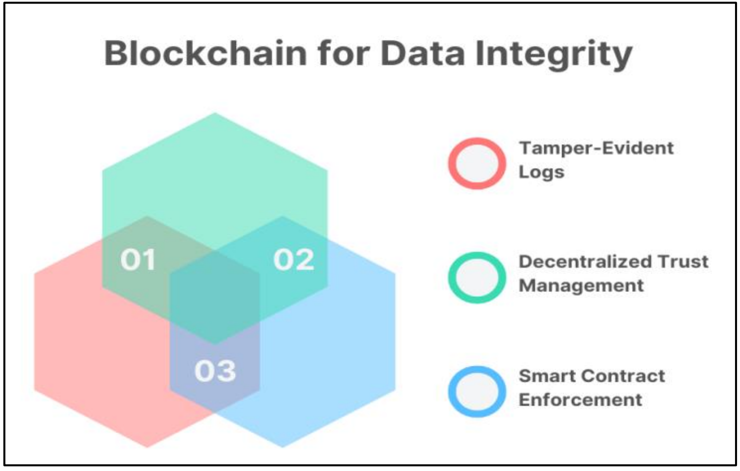
Blockchain for Data Integrity
01
02
03
Tamper-Evident Logs
Decentralized Trust Management
Smart Contract Enforcement

Figure 4. Blockchain for Data Integrity

- **Tamper-Evident Logs:** The integrity of data is achieved by creating tamper-evident logs using blockchain technology. [15-19] Every transaction or data set is put into a cryptographically tied block, which constructs a chain such that it would be a difficult task to tamper with any single block of transactions, as it would need to alter every block afterwards, a fact that is computationally impossible. This unalterability guarantees that modified records cannot be tampered with, and any form of unauthorized or abuse is easily identified; thus, a blockchain is phenomenal in keeping audit trails and forensic records of sensitive systems such as an ERP and critical infrastructure.
- **Decentralized Trust Management:** Decentralized structure is one of the characteristic features of blockchain and the solution to central authority management of trust. With the traditional system, a single node or administrator can compromise the data integrity of all nodes. Blockchain decentralizes this trust to a group of nodes and can be validated employing consensus algorithms (such as Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. The overall effect of such a decentralized version of trust is increased resilience, decreased single points of failure, and increased transparency in collaboration scenarios using multiple stakeholders.
- **Smart Contract Enforcement:** Smart contracts represent a form of program that is executed automatically once a set of predefined rules and agreements is satisfied and is stored on a blockchain. Within data integrity and data security, policies like data access, checking, or even workflows and people belonging to different organizations can be automated with smart contracts. The smart contracts also lower the risks of human error because the rules are directly integrated into the code, and no unauthorized actions can be taken; all the operations are performed in a secure and verifiable.

3.4. Role-Based Access Control (RBAC)

One of the access management models that has gained popularity is Role-Based Access Control (RBAC), which limits the access of a system according to the role of the users in an organization. In contrary of the approach mandating the administration of a set of privileges to each specific user, RBAC organizes sets of privileges by roles which are in turn assigned to individuals depending on their roles and duties. Under this direction, managing access rights becomes more straightforward, and security improves because it puts the principle of least privilege into practice, allowing it to ensure compliance with regulatory standards. To illustrate this in an ERP system, a user with an HR role, such as HR Manager, might have access to employee records and payroll modules, whereas a user with a role of Finance Officer may only have access to financial transactions and reporting tools. Well-defined roles will help such organizations to reduce the possibility of unauthorized access or privilege escalation. RBAC is particularly applicable in large and complex systems, such as enterprise and critical infrastructure systems, where it would not be practical to administer individually granted user permissions. It accompanies organizational policies by providing access rights as per the operational requirements of a user. It can be combined with an identity management solution to automate the role assignment process according to the employee's attributes.

Nevertheless, in its turn, despite the advantages, the RBAC is not suited to dynamic or fluctuating situations. With roles changing and their intersections, it is increasingly challenging to maintain clear roles and their definitive meanings, and it is even more difficult to update permissions. There, security and efficiency may be compromised by role explosion (an excessive number of roles) or by role drift (incorrect mapping of roles). To reduce these complications, certain organizations have expanded RBAC by including further versions of it, like Attribute-Based Access Control (ABAC), to incorporate other elements like time, place, or device into the rulemaking. However, RBAC is a basic access control model due to its understandability, ease of auditing, and effectiveness in applying standardized security policies to applications and systems. In an ERP and networked environment, RBAC, when well-managed, can greatly mitigate insider threats and serve regulatory compliance.

4. Results and Discussion

4.1. Test Environment

To assess how cybersecurity measures prevent risks to the protection of ERP systems, a controlled test environment was designed based on the simulated deployment of the SAP ERP. The environment was set on a segmented net, which was built to provide a closer resemblance to real-life enterprise architecture layouts. The segmentation involved specific areas, including internal users, external users, database servers, application servers, and those related to monitoring systems, so that the means and ways of communication flows were properly interpreted and controlled, along with the attack surfaces. This was vital in modelling realistic attack vectors and implementing containment measures under test conditions due to the network isolation. The common enterprise functions represented by the SAP ERP system are outfitted with standard modules like Finance (FI), Human Capital Management (HCM), and Materials Management (MM), which normally store sensitive and mission-critical information that requires protection due to its potential to cause loss and harm when compromised. In this context, the attacks, as well as the defence scenarios, have been implemented to reproduce real-life cybersecurity events. Some of the simulated attacks in the scenarios involved regular attacks, including phishing, credential harvesting based on maritime systems, SQL injection against various web-facing components, brute-force attacks against access portals, and attempts to gain privileges through misconfigured roles, among others. These attacks were initiated using dedicated attacker nodes placed in external network zones to provide a representation of the threat landscape that the real-world ERP implementations experience. On the defensive side, the setting had multi-layered security measures such as firewalls, intrusion detection/prevention systems (IDS / IPS) and integration with SIEM to serve as real-time monitoring and notification tools.

Furthermore, high-tech solutions, such as AI-powered anomaly detection and blockchain-based data integrity modules, were trialled alongside conventional security tools to compare their effectiveness in early detection and response to potential threats. Policies related to access were also applied, including Role-Based Access Control (RBAC) and Zero Trust Architecture, which restrict lateral movements and provide contextual verification of access requests. The system behavior was determined by collecting and analyzing logs continuously in a manner that determines the vulnerability of the system, besides ensuring that every security control is effective.

4.2. Performance Metrics

Table 1. Performance Metrics

Metric	Without Model (%)	With Model (%)	Improvement (%)
Detection Rate	65%	93%	28%
Incident Response Time	100%	33%	67%
Data Integrity Violations	100%	13%	87%

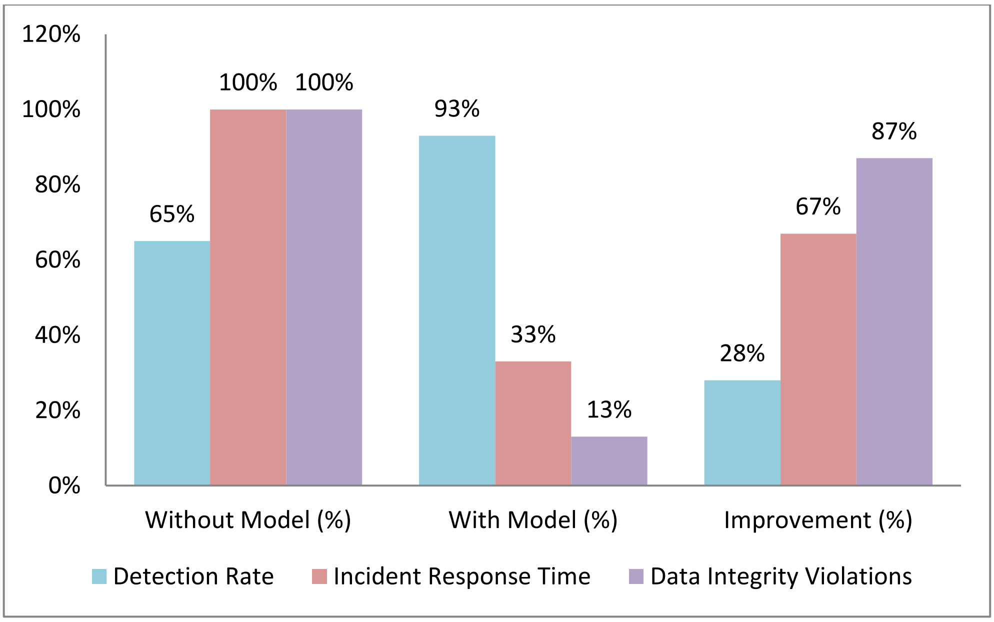

Figure 5. Graph representing Performance Metrics

- **Detection Rate:** The detection rate is the system's capability to detect and flag malicious activities. In the absence of a proposed security model, the ERP system was barely detecting 65 per cent of the threats, indicating that more than a third of the threats were not detected. The rate of 93 per cent was achieved following the implementation of a multi-layered model that incorporated the use of AI-based anomaly detection and Zero Trust principles. This indicates a 28% gain, implying that the degree of threat visibility is significantly higher, and the model can identify both known and unknown attacks with greater precision.
- **Incident Response Time:** Incident response time is the parameter which characterizes the swiftness of detecting the security threat, its analysis and the response. Under the first arrangement, the mean response time was 120 minutes, which corresponds to 100% baseline effort. This improvement reached 67 percent, as the new model helped reduce the response time by two-thirds of the previous time, to approximately 40 minutes. This can be significantly reduced by monitoring in real-time through Click-and-SIEM integration and other methods, such as applying AI to analyze alerts more rapidly and take automatic responses. Faster reaction time plays a significant role, as it severely restricts the amount of damage and the cost of reconstruction in the event of an attack.
- **Data Integrity Violations:** Data integrity violations denote those cases in which data was changed or corrupted in unauthorized way. The baseline environment, with no model enhancement, logged 15 violations, which is pegged at 100 per cent. Having implemented blockchain-based tamper-evident logging and tightened access control, the number of violations was reduced to only 2 instances, which constituted 13 per cent of the initial number and represented an 87 per cent decrease. Such a decrease in numbers attests to the functionality of blockchain and audit-related systems in ensuring the validity, credibility, and integrity of essential ERP information.

4.3. Discussion

The multi-layered cybersecurity model (implemented in the ERP test environment) proved that there has been considerable improvement in threat detection, the effectiveness of responding to the threats, and the integrity of data. The topic that had the most significant impact was the implementation of Artificial Intelligence (AI) within the Intrusion Detection System (IDS). One of the main criticisms of traditional IDS implementations is that most of them produce large quantities of false positives, which tend to overwhelm the security liaisons and hinder actual responses. The separation of dangerous activity and legitimate activity was improved by integrating AI-powered behavioral analytics into IDS so that the latter was more capable of identifying the presence of a genuine threat. Not only did that decrease the number of false alarms, but it also increased the confidence in received alerts, resulting in more focused and timely action. Blockchain technology played a crucial role in protecting system logs and ensuring the integrity of recorded events. In traditional systems, it is possible to alter or erase logs used to track attackers, thereby destroying any possibility of forensic investigation or accountability. By creating tamper-evident and immutable logs using blockchain, all transactions or events that occur within the system are permanently stored on a decentralised ledger. This unchangeability ensures that any effort to alter the previous records will become instantly noticeable, thereby enhancing auditability and confidence in the data, both during compliance checks and in breach inquiries. RBAC was also an invaluable protection measure against the insider threat, which is one of the most significant issues in cybersecurity. Using strict and job-specific assignment of permissions, RBAC greatly reduced the possibilities of the unauthorized access to sensitive ERP modules by enforcing the principle of the least privilege. Practically, this implies that once the credentials of an internal user are compromised, an attacker will only have access to non-essential functions. All these technologies worked together synergistically to form a robust security system that can adapt to changes in any aspect of security, while ensuring the usability of systems and ensuring system compliance with organizational policy.

4.4. Challenges

Although the multi-layered security model has achieved significant gains, several issues have arisen during its implementation, particularly with legacy ERP systems. Among the greatest challenges was integrating modern security elements, including AI-based anomaly detection and blockchain logging, with the existing SAP ERP infrastructure. Legacy systems are known to be rigid, with outdated architectures that do not easily support newer technologies. Compatibility problems have followed, with wide-ranging customization and development of middleware involving many efforts to establish a connection between modern tools and more traditional software frameworks. Additionally, vendor support was limited, and system dependencies were complex, which made it cumbersome to introduce changes without jeopardizing the operation of the business. The other problem was that the computational overhead involved in AI modules was high. Although AI has enabled the detection of threats with such precision, it has also brought a heavy burden on system resources. The use of machine learning algorithms, particularly operations such as deep learning or real-time behavioural analytics, requires specific memory assignments and computational processing capabilities. This was particularly a problem where the ERP systems were already operating near capacity. This would compel organizations to consider infrastructure upgrades or offloading the AI work to cloud-based services, neither of which comes without an added cost and complexity. The challenge was also posed by users who rejected new security measures, primarily multifactor authentication (MFA). Although MFA provided an important additional layer of protection, it solved the problem at hand, as it was intrusive or inconvenient to many users, especially when using ERP systems frequently during the day. Such disliking would result in delays in adoption or even bypassing of security measures, and the intended protection grounds are therefore compromised. It was paid to overcome this not only by technical means, such as more efficient authentication applications or biometrics, but also by educating and managing change and acceptance. These pitfalls teach us that balance must be found between security and usability, and that the technological upgrades should coincide with the operating capacity as well as organizational culture.

5. Conclusion

The offered cybersecurity model is an elaborate, multi-level framework designed to address the emerging threat environment that is ravaging ERP systems in the national critical infrastructure (NCI). The model integrates conventional security measures with advanced technologies, including Artificial Intelligence (AI), blockchain, and Zero Trust concepts, to provide enhanced security against most attack vectors, including insider threats, phishing, ransomware, and data tampering. The layered nature of the approach will also enhance visibility, control, and resilience, as a single point of failure cannot bring the system down. The overall approach is not only better at defending the entire security posture of ERP environments but also aligns with best practices in present-day cybersecurity architecture.

The study brings some novelty to the study of ERP security. To begin with, advanced and covert threats that previous security tools inadequately detect can be spotted far better with the inclusion of behavioral anomaly detection AI, which can be used comprehensively. Upon studying usage patterns, AI can be used to detect deviations in real-time and launch corresponding responses earlier. Second, blockchain technology is utilized to protect logs and transactional information, ensuring they are tamper-evident and have forensic traceability. This increases trust and integrity in ERP systems tremendously. Third, the model further enforces access control using Role-Based Access Control (RBAC) and suppresses escalation of privileges as well as minimized the success rate of insider attacks. These technologies, combined, form a massive and flexible platform that can cater to both existing and emerging challenges in the sophisticated environment of enterprises.

Going forward, some improvements can be made to strengthen the proposed model. One such point is the introduction of quantum-resistant encryption algorithms to equip ERP systems against risks posed by future quantum computing, as quantum computers may theoretically break existing cryptographic standards. The second direction is the integration of real-time threat intelligence feeds, ensuring the system remains current with the faces of global threats and is sufficiently adaptive to new attack signatures and indicators of compromise. Finally, a compliance mechanism that aligns with international standards, such as ISO/IEC 27001, would provide continuous assurance and simplify regulatory audits. Not only would this decrease manual overhead, but it would also help with proactive risk management, as current operations can be aligned with established frameworks. These developments would render the model even more sophisticated, future-ready, and suitable for implementation in highly sensitive and regulated areas.

References

[1] Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014, May). Understanding insider threat: A framework for characterizing attacks. In 2014, IEEE Security and Privacy Workshops (pp. 214-228). IEEE.

[2] Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). Cybersecurity of critical infrastructures: Challenges and solutions. Sensors, 22(14), 5105.

[3] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.

[4] Stafford, V. (2020). Zero trust architecture. NIST special publication, 800(207), 800-207.

[5] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278-1308.

[6] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[7] National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST, April 16, 2018.

[8] Nwafor, M. C., Okezie, C. C., & Azubogu, A. C. O. (2018). Design and Implementation of a Multi-Layered Security Enterprise Resource Planning (ERP) System for Mission Critical Applications. J. Comp. ICT, 11, 71-84.

[9] Chinta, P. C. R. (2020). A Deep Learning Architecture for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. Journal of Artificial Intelligence and Big Data, 1(1), 10-31586.

[10] Goel, S., Kiran, R., & Garg, D. (2012). Vulnerability management for an enterprise resource planning system. arXiv preprint arXiv:1209.6484.

[11] Moore, C. (2023). AI-powered big data and ERP systems for autonomous detection of cybersecurity vulnerabilities. Nanotechnology Perceptions, 19, 46-64.

[12] Ashraf, H., Alenezi, M., Nadeem, M., & Javid, Y. (2019). Security Assessment Framework for Educational ERP Systems. International Journal of Electrical and Computer Engineering, 9(6), 5570.

[13] Hong, J. B., & Kim, D. S. (2016). Towards scalable security analysis using multi-layered security models. Journal of Network and Computer Applications, 75, 156-168.

[14] Khan, M., Naz, T., & Medani, M. A. H. (2019). A multi-layered security model for a learning management system. International Journal of Advanced Computer Science and Applications, 10(12).

[15] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143-57179.

[16] Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer Security Incident Response Team Development and Evolution. IEEE Security & Privacy, 12(5), 16-26.

[17] Chen, L. (2011). Analyzing and developing role-based access control models (Doctoral dissertation, Royal Holloway, University of London).

[18] Mishra, A. P., Dublish, M., & Kumar, D. (2022). Cybersecurity application in ERP implementation. J. Pharm. Negat. Results, 13, 2507-2522.

[19] Khan, S., Parkinson, S., & Crampton, A. (2017, December). A multi-layered cloud protection framework. In Companion Proceedings of the 10th International Conference on Utility and Cloud Computing (pp. 233-238).

[20] ISO/IEC. ISO/IEC 27001:2022 — Information technology — Security techniques — Information security management systems — Requirements. ISO, 2022.

[21] Thirunagalingam, A. (2022). Enhancing Data Governance through Explainable AI: Bridging Transparency and Automation. Available at SSRN 5047713.