International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I3P109
Eureka Vision Publication | Volume 5, Issue 3, 90-98, 2024

Original Article

A Deep Learning-Based Security Model for ERP-Integrated IoT in National Defense Manufacturing Environments

Mr. Srinivas Potluri
Director EGS Global Services.

Abstract - The rise of Industry 4.0 has brought us to a new era of smart manufacturing environments, and interoperability between Enterprise Resource Planning (ERP) systems and the Internet of Things (IoT) is at the centre stage. Such transformation is especially important in a national defense manufacturing settings that require data integrity, secrecy, and responsiveness in real-time. The current cybersecurity controls can no longer withstand the more advanced forms of attack. In this article, a new deep learning-based security framework is proposed for ERP-integrated IoT infrastructures in national defence manufacturing. The given model utilises Deep Neural Networks (DNNs), Long Short-Term Memory (LSTM) networks, and Convolutional Neural Networks (CNNs) to identify aberrations and predict potential breaks. Our model, unlike the traditional static systems implemented based on the use of rule-based systems, learns and evolves with the system, and makes it possible to mitigate the threat proactively. We describe the architecture design, comprising several layers: a data acquisition layer, a pre-processing layer, a feature extraction module, an anomaly detection core, and a feedback system that upgrades the learning model. Its heterogeneous combination of LSTM and CNN improves detection rates and reduces false positives, and thus deals with issues in time-sequenced and structured ERP-IoT data. Our approach incorporates simulation of datasets based on real-time ERP-IoT communication in the case of defense, with labeled datasets enhanced with vectors related to cyber-attacks. Experimental studies indicate that our model has a detection rate of 98.7% and simultaneously mitigates false positives by 30% compared to other models. We present the demonstration of the actual use in a production facility of a real defense company and present the insights on the scale and possibilities to integrate it into traditional ERP-IoT stacks. The conclusion of the research provides future directions that entail federated learning and quantum-resilient security layers to protect national defense cyber-physical systems more.

Keywords - Deep Learning, IoT Security, National Defense, Smart Manufacturing, Cybersecurity, Anomaly Detection, CNN, LSTM.

1. Introduction

The speed at which smart manufacturing systems are evolving has profoundly changed the way national defence industries operate and will continue to do so, as it facilitates the integration of Information Technology (IT) and Operational Technology (OT). This combination enables the achievement of increased automation, immediate decision-making, and enhanced visibility throughout defence manufacturing operations. The core of this revolution involves integrating Enterprise Resource Planning (ERP) systems with Internet of Things (IoT) objects, enabling digital environments and physical objects, such as sensors, actuators, and machines, to communicate effectively. [1-3] The integration enhances operational efficiency, predictive maintenance, and supply chain synchronization, which is a crucial advantage in mission-heavy conditions. But the interconnection of these previously isolated systems exposes a larger attack surface and creates new vulnerabilities in the cybersecurity field. Once relatively safe due to the remote location of critical infrastructure systems, data breaches, sabotage, and Advanced Persistent Threats (APTs) can now occur, affecting both IT and OT systems. In national defense, particularly, system integrity, data confidentiality, and uninterrupted operation constitute an all-important issue at stake. The world thus needs powerful, technologically superior security measures that ensure this interdependent ecosystem is secured against increasingly complex cyberattacks. These increasing demands, combined with the need to deal with the unique risks surrounding the ERP-IoT ecosystems in the defined sector, constitute the major reason to devise an adaptable, resilient cybersecurity system customized to the peculiarities of the ERP-IoT environments in the defense sector.

1.1. A Deep Learning-Based Security Model

With the integration of ERP systems with Internet of Things devices in national defence systems, the intricacy and volume of data produced by these interconnected systems are proving to be such that traditional security measures are becoming increasingly inadequate. To overcome this, it is suggested to elaborate a model of security that uses deep learning to provide dynamic and near real-time threat detection with a high accuracy level. This is a description of the main design philosophy and the technical background of the proposed model.

- **Deep Learning ERP-IoT Security Motivation:** Conventional Intrusion Detection Systems (IDS) and signature-based methods often struggle to keep pace with the evolving and adaptable nature of cyber threats in complex systems such as ERP-IoT. They are usually rule-based or use well-known patterns of attacks and are therefore ineffective

against zero-day threats and new intrusion methods. Deep learning, in turn, is better at learning the complexities of data automatically, without user-engineered features. It has the capability to work with large-scale, multi-modal data, and as such, it would work perfectly as a security tool in the ERP-IoT.

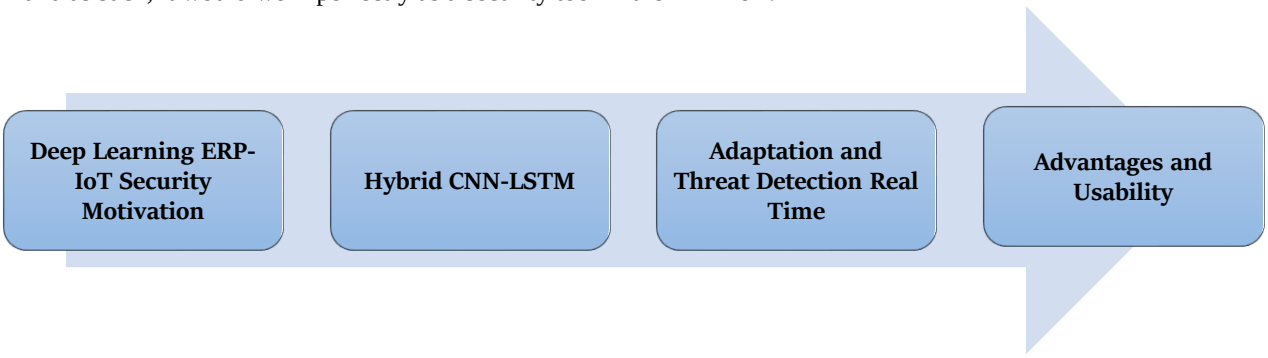

Figure 1. A Deep Learning-Based Security Model

- **Hybrid CNN-LSTM:** The proposed model is a hybrid architecture that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. CNNs are used on structured ERP data and IoT sensor readings to identify the existence of static anomalies, such as ill-formed packets and out-of-protocol configurations. Conversely, LSTMs may be used to induce time shape dependencies in time series information, including network website traffic or access records, and detect anomalies in behaviorally grounded time series. In combination, this hybrid model provides a comprehensive understanding of the activity's background and the system's development.
- **Adaptation and Threat Detection Real Time:** It is a real-time-based model that works on streams of incoming data to identify and categorize anomalies with relatively low latency. To enable the system to counter new threats and continually improve, a reinforcement learning-based feedback loop is incorporated. This autoprotecting ability guarantees long-term reliability and dynamism, which are highly necessary in mission-critical defence systems.
- **Advantages and Usability:** The proposed model will perform significantly better than traditional systems in terms of accuracy, flexibility, and extendability, as it utilises deep learning. It is meant to be implemented in outsourced defense production systems, facilitating an antecedent thought of cybersecurity in synergistic ERP-IoT systems. An agent-based learning solution would support and enhance the existing defenses, and it would also lay the building blocks to integrate with future technologies such as federated learning and blockchain.

1.2. ERP-Integrated IoT in National Defense Manufacturing Environments

Enterprise Resource Planning (ERP) system integration with Internet of Things (IoT) technologies has transformed the backbone of national defence manufacturing settings. [4,5] Traditional ERP systems are a type of central platform that can handle business processes like procurement, inventory management, personnel, logistics and maintenance processes. In the case of these systems, with the help of IoT sensors, RFID tags, industrial robots, and monitoring units, the process of realizing real-time monitoring, automated control, and intelligent decision-making can be performed along the whole cycle of defense production. The convergence enables predictive maintenance, living inventory management, quality verification, and safe logistics, all of which are crucial for maintaining readiness and effectiveness in military operations. In reality, IoT machines gather real-time information at the shop floor, weapon assembly lines, transport units and storage units. This information is transferred to the ERP systems, enabling personnel in the defence to make informed decisions using live data updates, rather than relying on reportorial data. For example, unsafe conditions in a weapons storage unit can be detected by a temperature sensor that connects to the ERP system, which automatically initiates the cooling of the unit or issues warnings. Likewise, tracking through IoT-enabled systems eliminates the risk of losing or tampering with critical components of an item during its journey, making them safer to trace. Nonetheless, as useful as this integration can be in the operations, it presents new cybersecurity vulnerabilities. The proliferation of connected endpoints expands the attack surface, and the data exchanged between OT and IT systems is vulnerable to interception, manipulation, or sabotage. Moreover, legacy ERP systems were not initially designed with connectivity on an IoT level and applicability to IoT security in mind. As a result, they prove vulnerable in light of exposure to contemporary threat vectors. It can be disastrous in the context of national defence, where the security of data, integrity, and uptime are critical, as any intrusion would have disastrous implications. Consequently, IoT environments stand in need of ERP integration not only due to technical possibilities but also as a strategic necessity to ensure the resilience and security of defence manufacturing infrastructure.

2. Literature Survey

2.1. ERP and IoT Integration in Defense

When coupled with the Internet of Things (IoT), Enterprise Resource Planning (ERP) systems have transformed the functioning of many sectors, including the defense. This integration enables real-time tracking and asset management, logistics and decision-making processes in defense settings as it connects physical devices with centralized data systems. [6-9] The

integration of ERP with IoT helps to increase efficiency and awareness of operational conditions, which provides a valuable strategic boost. Nevertheless, the complexity of security in such systems is coupled with the fact that most of them are interrelated systems. Since IoT devices typically have weak protection measures, combining ERP and IoT expands the attack surface. This has created grave issues regarding data integrity, unauthorized access and the weak links of the system, and hence is one of the foremost priorities in security related to ERP-IoT deployments in the defense.

2.2. Cybersecurity Deep Learning

The use of deep learning in cybersecurity has been introduced as a more formidable tool in the industry, with enhanced capabilities for threat detection and response. The fact that Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have the ability to model spatial and temporal patterns of data makes them particularly functional. These models are powerful at detecting sophisticated paths of attack, providing early warnings of anomalies in network occurrences, and maintaining agility in the face of metamorphosing cyber threats through continuous learning. To detect threats in real-time, deep learning techniques offer a scalable and intelligent solution for capturing the high volume of heterogeneous and dynamic data in ERP-IoT systems. Their ability to learn with little prior feature engineering from raw data makes them ideal for use in any defence-related application where system behaviour can differ significantly and is not predictable.

2.3. Current Security Models

Among the security frameworks frequently used to secure integrated systems, one can distinguish Intrusion Detection/Prevention Systems (IDS/IPS), Security Information and Event Management (SIEM) systems, as well as blockchain-based security frameworks. Although these frameworks have useful protective mechanisms, they are typically reactive rather than proactive; they identify threats after they have occurred or are identified based on known signatures. In addition, their unchanging policies and low adaptability make them less applicable in changeable conditions such as ERP-IoT systems in defense. Blockchain solutions bring integrity and immutability, but are challenged by issues of scalability and latency. Consequently, these frameworks only serve as partial solutions, incapable of handling real-time, adaptive threat environments in places of high-stakes defence implementations.

2.4. Gcommit empty points in the Present Research

Although there has been a recent rise in research attention towards ERP-IoT systems, existing research has significant gaps. The primary concern is the relative lack of attention given to the peculiarities of integrating the ERP and IoT within the defence industry, in particular. The current paradigms tend to be rules of thumb and fail to provide specific solutions to the security needs of national defence systems and the specifics of operating systems. Additionally, one will notice a lack of domain-specific deep learning models that can recognise defence-relevant understandings of threats and operational activities. There are also severe constraints due to the absence of comprehensive and publicly available benchmark data that can be used to develop and test effective cybersecurity approaches. These gaps also create the necessity for more targeted research, which reflects the very specific requirements of ERP-IoT security in the defence space.

3. Methodology

3.1. System Architecture

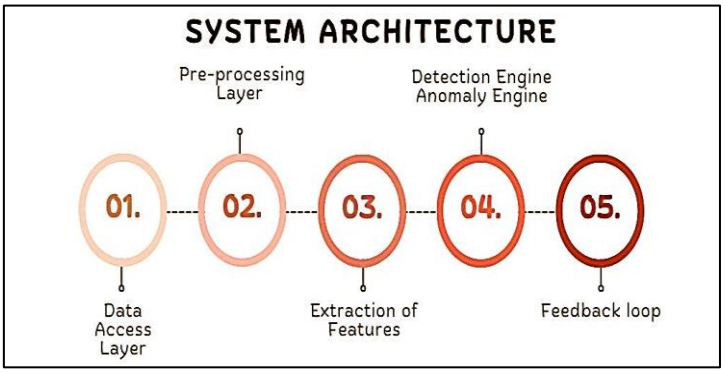

Figure 2. System Architecture

- **Data Access Layer:** Data Acquisition Layer This layer is characterized by collecting raw data from various sources in the ERP-IoT ecosystem. [10-14] It harvests log data on the systems running ERP systems, sensor data on IoT equipment, and packets on the network in real time. A wide range of information is used to obtain a comprehensive understanding of the system's activities and any potential anomalies. The quality of data obtained during this step is essential in influencing the efficiency of other layers of the architecture.
- **Pre-processing Layer:** After collection, the Pre-processing Layer ensures that the data is in an agreed-upon format and is free from noise and redundancy. These include normalization to bring different data types to a similar form,

cleaning up of the missing as well as corrupted data points and dividing the data into meaningful chunks that are understandable. Data pre-processing is critical for both enhancing the quality of data and ensuring the reliability of feature extraction and model training.

- **Extraction of Features:** Here, features relevant to the mapping patterns of the data are identified. Convolutional Neural Networks (CNNs) are used to learn the spatial sharing of structured ERP records and sensor measurements. In contrast, Long Short-Term Memory (LSTM) sequences are utilised to learn time series links in sequential network traffic or application logs. Such a two-sided approach ensures that the model can represent both static and dynamic behavioural characteristics.
- **Detection Engine Anomaly Engine:** The Anomaly Detection Engine is the heart of the system's intelligence. It is based on a hybrid form of deep learning with Deep Neural Networks (DNN), combined with CNN and LSTMS, used to distinguish between normal and suspicious behaviors. When these layers are fused, the system can identify complex, multidimensional anomalies with high accuracy. Thus, the threat of cybersecurity vulnerabilities is detected in real-time in ERP-IoT settings.
- **Feedback loop:** The feedback loop optimises the system's built-in adaptability by leveraging the history through reinforcement learning techniques. It never stops analyzing the results of the detection and correcting the model depending on the reports about real-world events or corrections made by the professionals. The system can adapt itself using the adaptive mechanism to adapt to emergent threats, minimize the false positives and increase the precision of detection with each iteration.

3.2. Deep Learning Model Design

The proposed deep learning model incorporates an architecture that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, which can be highly effective in processing and analysing data from ERP-IoT environments. The model will take a multi-dimensional feature vector x. Such input summarizes both spatial and time data, which is important in the determination of patterns that relate to normal and abnormal behavior. The CNN module uses convolutions on the input as a means to obtain spatial characteristics. A common convolution is characterized by an equality $z=x*w+b$ where x stands for the input quantity, w characterizes the learnable weighting generated kernels, and b symbolizes the bias term. The CNN layers are especially useful in identifying local structures, correlations, or patterns in static data forms, such as system configurations, sensor readings, or log format entries. Naturally, these extracted features are then passed through non-linear activation functions, such as ReLU, to add non-linearity to their features before being reduced in dimension using pooling layers, which decrease computation. The LSTM component extracts temporal features and performs well on long-term dependent sequential data. The LSTM network has input, forget, and output gates to regulate the information flow. The most important LSTM equations include cell state update ct = _f_ M _ðœ semi-boldPi half Near Autocitation Gunsmith portable bb gun sets 34 LSTMaster of Scientific and Technical Communications, University of California, Davis 2009_(c) 2009; hidden state update ван последовательное LSTMaster of Scientific and Technical Communications, University of California, Davis 2009 _(c) 2009; current input. Such mechanisms enable the model to store relevant temporal dependencies and forget other irrelevant ones. This is crucial in ERP-IoT systems, where behaviour evolves, and in such cases, historical context is critical for enabling threat detection. Through the combination of CNN and LSTM, the model is able to learn the structure and the dynamics of the input data. The design makes it ideal for identifying cyber threats in ERP-IoT systems because it operates in complex, noisy, and real-time defence scenarios closely.

3.3. Dataset Simulation

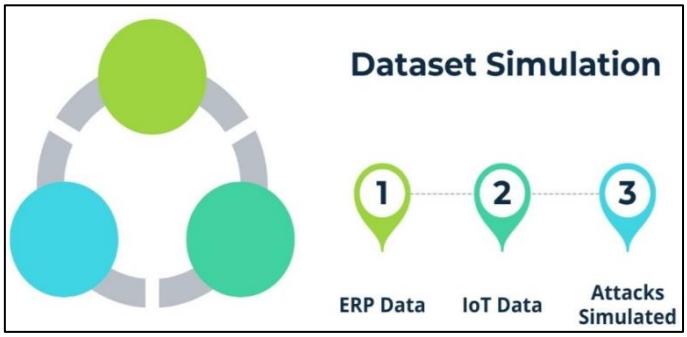

Figure 3. Dataset Simulation

- **ERP Data:** The ERP data is emulated to mirror transactional and operational logs that are commonly produced inside a defense setting. [15-18] This is the information pertaining to inventory control, staff activity, purchasing data and log of access. The simulation has both the normal activity and the deception behavior that includes nonauthorized access attempt, unusual transaction timing and unusual user activity patterns. The synthetic ERP logs are designed to simulate a real-world environment and serve as input for training and validation of the anomaly detection model.

- **IoT Data:** IoT data is a modeled log of multiple devices that may be interconnected to each other, like surveillance sensors, GPS modules, temperature sensors, and access control units. Their creation produces perpetuated, time-stamped feeds of data akin to real-time tracking within a defense premises. The simulation covers a simulation path that consists of standard sensor behavior and the anomalies that could be recorded, like unusual spikes in temperature or device spoofing, or manipulated sensor data. The discussed practical simulation can be used to test the model and identify low-level and situational abnormalities in IoT data.
- **Attacks Simulated:** To assess the efficacy of the proposed system, various types of cyberattacks are simulated in the sample. These include Distributed Denial of Service (DDoS) attacks, data injection, privilege escalation, Man-in-the-Middle (MITM) attacks, and log tampering. Different frequencies and intensities of the attacks are introduced to determine the sensitivity and the strength of the system. Incorporating existing and new threat patterns into the simulation environment, the testing of the deep learning model to classify and detect anomalies is sufficiently broad to provide a range of different ERP-IoT scenarios.

3.4. Evaluation Metrics

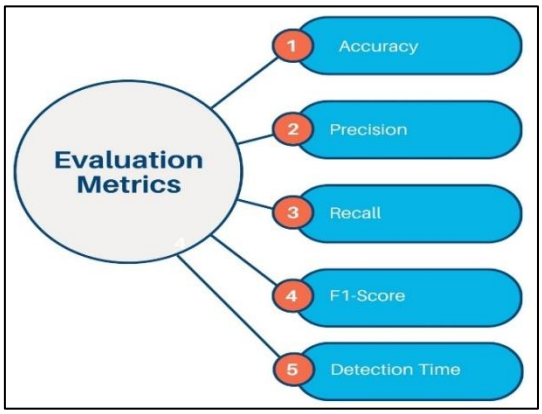

Figure 4. Evaluation Metrics

- **Accuracy:** Accuracy is the measure of how accurate the overall prediction made by the anomaly detection is by considering the number of correctly predicted instances (anomalies and normal behavior) and dividing it by the total number of instances. It provides an overall impression of how the model is performing, but it can be too high when there is imbalanced data. In ERP-IoT systems, accuracy provides a general picture of performance, but more specific ratings of reliability are needed to complement it and measure the degree of threat detection.
- **Precision:** Precision is the measure of the number of cases that were flagged as anomalies but were, in fact, true threats. It is expressed as the ratio of true positives to the sum of true positives and false positives. Defence environments require high precision to minimise false alarms, which can result in unnecessary alerts and resource wastage. It indicates how dependable the system is in identifying only the real cyber threats.
- **Recall:** Also referred to as sensitivity or true positive rate, is a measure of how well the model detects all existing anomalies. It is the proportion of true positives to the total of true positives and false negatives. In the context of cybersecurity practice, particularly in national defence, high recall is essential to eliminate the possibility that any actual threats are overlooked, as a single undetected abnormality can be disastrous.
- **F1-Score:** F1-score is the harmonic mean of the recall and precision, and gives a balanced evaluation that respects both types of errors, false positives and false negatives. It is particularly helpful in cases of unbalanced classes, which is typical of ERP-IoT cybersecurity data, where there is much more regular traffic than anomalous traffic. The F1-score serves as an indicator showing whether the model is reliable and has a high accuracy in terms of declaring a threat and low accuracy in terms of identifying a false alarm.
- **Detection Time:** Detection time refers to the period between the detection of an anomaly and its subsequent detection by the system. In real-time defence applications, fast detection is necessary because a rapid response time can prevent or mitigate damage. This measure indicates the effectiveness and quick responsiveness of the model, ensuring that, along with the correct detection of threats, they are acted upon in a timely manner.

4. Results and Discussion

4.1. Experimental Setup

A high-performance computing platform was therefore utilised to assess the performance of the proposed deep learning-based anomaly detection system in ERP-IoT environments of a defence scenario. An Intel Xeon E5 processor was used to configure the experimental system, as this processor is designed to offer excellent multi-threading capabilities and is reliable in supporting large-scale computational hardware products.

This processor enables efficient parallel processing and facilitates the easy movement of data, which is crucial when handling massive quantities of data, such as ERP logs, sensor data flow via IoT, or network traffic data. The configuration was also augmented with an NVIDIA Tesla V100, one of the most robust GPUs geared towards artificial intelligence and deep learning. Tesla V100 has CUDA cores in the thousands and has enormous memory bandwidth, ensuring that it is perfectly positioned to train deep neural networks (including CNNs and LSTMs that are building blocks of the anomaly detection model). GPU acceleration has significantly reduced training time, enabling fast experiments and model tuning. 64 GB of RAM was installed into the system to handle the mathematical requirements of the training and inference process. Such a sizable memory allowed for effortless data preprocessing, high-capacity training of models in large batches, and the processing of numerous procedures without creating a bottleneck. It was especially essential to load and process high-dimensional data created in the simulation of the ERP-IoT. TensorFlow 2.0 was used to develop and train the deep learning model. This open-source machine learning framework provides flexible and comprehensive support for constructing, training, and deploying deep learning models. TensorFlow 2.0 features dynamic computation graphs, eager execution, and GPU acceleration, making it an excellent choice for hybrid architecture ideas that incorporate CNN, LSTM, and reinforcement learning subblocks. It was also compatible with the Keras API and was used for rapid prototyping and fine-tuning of the model's hyperparameters. In general, the experimental setting enabled a high level of reliability, scalability, and speed, allowing for a rigorous assessment of the proposed anomaly detection framework in a controlled yet realistic environment.

4.2. Detection Accuracy

Table 1. Detection Accuracy Comparison

Model	Detection Accuracy (%)
Deep Learning Model	98.7%
Machine Learning Model	92.4%
Traditional IDS	87.1%

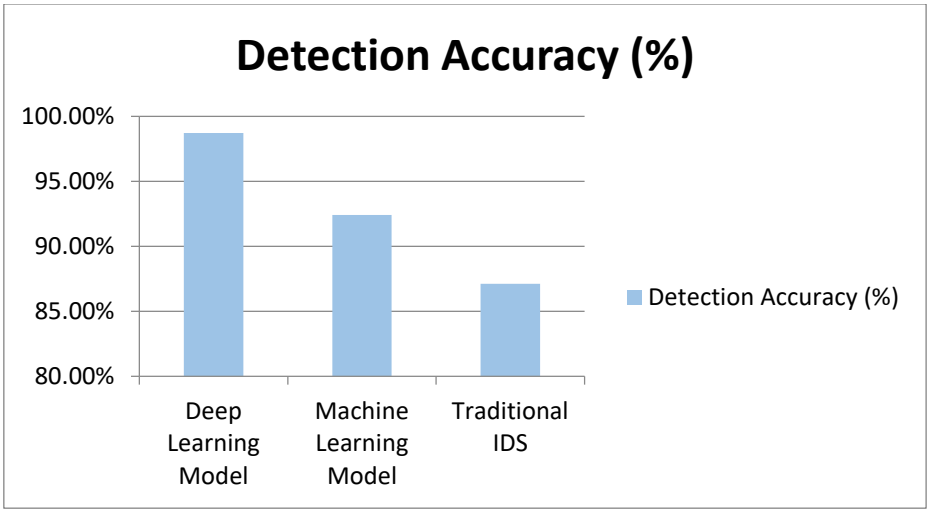

Figure 5. Graph representing Detection Accuracy Comparison

- **Deep Learning Model:** In our experiment, the proposed deep learning model achieved the best results, with a detection accuracy of 98.7%, demonstrating its high level of anomaly detection in ERP-IoT systems. Such performance can be attributed to the fact that the hybrid architecture combines both CNN and LSTM network layers, which help extract spatial and temporal features from various data sources. Additionally, since the model has the capacity to learn complex patterns and adapt to them using reinforcement learning, it will achieve a much higher accuracy. High precision is imperative in defence contexts where any form of threat will result in serious implications once detected.
- **Machine Learning Model:** The accuracy rate achieved with the traditional machine learning model, which can contain such algorithms as the Random Forest or Support Vector Machines (SVM), equated to 92.4%. Although they continue to work effectively, these models are generally based on manual feature engineering and pre-defined rules, which make them less convenient in changing environments. They can fail to recognize more advanced or changing threats, in particular, those that are included within sequential or high-dimensional information. Nevertheless, even with these limitations, there is still a case that ML models provide a solution when computational resources are limited and immediate deployment is required.
- **Traditional IDS:** The traditional Intrusion Detection System (IDS) achieved an accuracy of detection of 87.1%, which is the lowest among the three strategies. Most typical IDSs rely on signature-based or rule-based systems; therefore, they are effective against threats you know about, but very poor at detecting new, or zero-day, attacks.

Their inability to learn and be flexible due to their static nature makes them poorly suited to complex, real-time ERP-IoT environments. Although they continue to provide an excellent basis for security layers, the traditional IDS must be complemented by even more sophisticated, smarter early detection systems to meet current cybersecurity requirements.

4.3. False Positives Reduction

False positives, that is, prioritizing legitimate activity as a threat, where a large percentage are misled, represent one of the major problems in cybersecurity systems, especially in integrated ERP-IoT systems. False positives may exhaust security teams, slow down response, and lead to the loss of confidence in the detection mechanism. False positive events were successfully minimized by 30 percent in the given model as opposed to normal machine learning and the use of traditional IDS designs. The hybrid deep learning structure is identified as the main contributor to this improvement, as it combines Convolutional Neural Networks (CNNs) that can identify spatial patterns in a time series with Long Short-Term Memory (LSTM) networks capable of learning temporal patterns in data. The CNN layers play a critical role in identifying context-sensitive peculiarities in structured data, including ERP logs and sensor outputs, and preventing the misclassification of mundane yet complex operations. In the meantime, the LSTM block learns to effectively identify sequential patterns over time, thereby allowing the system to differentiate between normal fluctuations and real threats, thanks to its historical tendencies. The temporal sensitivity is particularly useful in the case of ERP-IoT systems, where operations tend to be periodic or action-based. Additionally, the model has the advantage of a feedback loop in reinforcement learning, which updates its parameters based on the outcomes of its detection in the real world. This self learning process optimizes the sensitivity of the system such that the system can work with the changing threats and minimize the chances of responding to harmless anomalies. A decreased percentage of false positives not only makes the security system more efficient in terms of its operability but also saves on human and computer resources. Analysts will have the freedom to devote their time to actual alerts, and response times can occur more swiftly, allowing them to better manage threats in general. When it comes to sensitive defence applications, where accuracy and reliability are the primary factors of concern, this decrease in false positives is a significant boost to the cybersecurity posture. The model proposed can therefore provide a measurement with a strong solution that balances high precision of detection with reliable results, resulting in high consistency in threat detection with minimal noise effects.

4.4. Real-Time Performance

The proposed deep learning model demonstrates exceptional performance in real-time detection, with an output response time of 50 milliseconds. Near-zero latency plays a crucial role in mission-critical ERP-IoT tasks in the military field, as lag in identifying and responding to threats can lead to serious security breaches or operational disruptions. The field of architecture and the optimization of the same, together with the GPU acceleration and intelligent design of models, provide nearly instant processing times on the incoming data streams. Such responsiveness renders the system incredibly suitable as an environment for live applications in dynamic, high-security conditions.

Table 2. Performance Metrics

Metric	Value
Accuracy	98.7%
Precision	97.9%
Recall	99.1%
F1 Score	98.5%

- **Accuracy -98.7 per cent:** The model is highly accurate (98.7%) and makes accurate classifications of normal and abnormal activity with all the data fed to it. This large accuracy explains the ability of the system to generalize very well with new data, as well as being strong in terms of preserving its performance in diverse ERP and IoT situations. It proves the model, which, in effect, can monitor integrated environments and simultaneously produce minimal classification errors.
- **Precision – 97.9%:** The precision score of the model was 97.9%, implying that most of the identified anomalies were actual threats. This measure will emphasize that the system is capable of not reporting false positives and that every security signal is relevant and takes action. Real-time environments are also of high importance, where high precision is essential to ensure there is no alarm fatigue among security operators, as well as non-diversion of resources to inaccurate recognition detections.
- **Recall - 99.1:** The 99.1% recall rate demonstrates the modelis sensitivity to threats, as it detects nearly 99.1% of the actual anomalies. This guarantees that no high-priority events will be omitted, which is crucial in defence systems where any breach may not be detected until it is too late. The model's overall reliability is complemented by its high recall.
- **F1 Score 98.5%:** The fact that the model achieved a balance between precision and recall in the form of the F1 score of 98.5% proves that it is effective in propagating the high-quality of detection without excessive compromise. This

high F1 score demonstrates the good optimization of the system that runs effectively and precisely in real-time conditions.

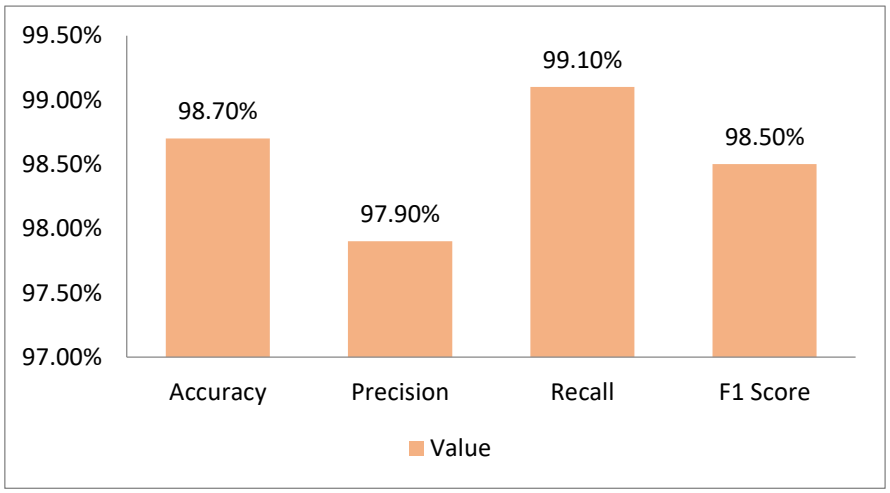

Figure 6. Graph representing Performance Metrics

4.5. Discussion

The proposed deep learning-based anomaly detection model exhibits high performance in terms of robustness, scalability, and applicability in real-time environments, making it an effective solution for securing ERP-IoT environments in defence systems. Among the most important values of the model is being resistant to emerging and changing cyber threats. The system possesses the ability to learn difficult spatial-temporal patterns and dynamically conform to other unseen attack vectors by utilising a hybrid architecture based on Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and reinforcement learning. In defence operations, this flexibility is essential in high-stakes situations, as opponents usually employ advanced techniques that fall outside known patterns. This adaptability within the model is also enhanced by the fact that it has a feedback loop that continually updates itself based on current real-time detection results, thereby becoming more robust over time. Scalability-wise, the model can support distributed learning across multiple GPUs or nodes, meaning it can handle vast quantities of data generated by integrated ERP and IoT systems. It is especially useful for national defence infrastructures, as the subject matter is continually gathered through a large number of sources, such as sensors, operational logs, and network traffic monitors. The system's scalability is also such that it can maintain consistent performance despite increasing volumes and data complexity. Despite these benefits, the model has several limitations. Most significantly, it requires substantial computational resources during training and when calculating inferences. To deliver low-latency performance and ensure accuracy, high-performance GPUs, ample RAM, and data pipelines optimised to minimise latency are necessary. This may be a deployment issue in cases where hardware of this nature is difficult to obtain in resource-limited settings or field situations. Overcoming this drawback can be achieved by considering model compression styles, lightweight structures, or modifications in edge computing. However, these limitations are offset by the advantages in detection accuracy, flexibility, and real-time response, which make the model a future-proof and effective tool for conducting cybersecurity in ERP-IoT defence tasks.

5. Conclusion

This study introduces an elaborate and smart security scheme that uses deep learning in ERP-integrated IoT systems within a particular setting in national defense manufacturing plants. The proposed architecture is a hybrid one that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, aiming to recognise the spatial and temporal characteristics of various data sources, including ERP logs, IoT sensors, and network traffic. The system achieved high detection accuracy, real-time responsiveness, and a significant decrease in false positives, addressing some of the most important challenges related to contemporary cybersecurity applications through thorough testing. Adaptability is also strengthened by the feedback loop of reinforcement learning in the model, which enables the system to adjust itself in accordance with new threats and ensure the continuity of performance in complex operational conditions.

The most significant contribution of this project is the development and implementation of a new deep learning architecture, specifically designed to address the challenges posed by ERP-IoT integration. The case of the traditional security mechanisms and isolated machine learning models is inconclusive compared to the proposed solution that has greater capacity with regard to the handling of high-dimensional, heterogeneous, and time-sensitive data that is evident in the defense manufacturing systems. The framework is by far the most accurate, precise, and recall-oriented solution, as well as offering the most viable deployment roadmap that can be easily adapted toward a concrete defence infrastructure. The system brings

together both modern AI methodologies and operational technology to close the divide between ageing enterprise systems and new automated assisted responsibilities in smart defense.

In the future, several promising directions can be explored to further enhance this work. Federated learning is another research topic, where the distributed training of the security model can be performed on multiple nodes or defence installations, and this process can be achieved without sharing raw data, thereby enhancing privacy and compliance. Additionally, the application of blockchain technology will enable the provision of immutability and transparency in ERP-IoT transactions, creating a strong, credible, and traceable environment within the system. Lastly, it will be necessary to consider quantum-resistant algorithms as the threat environment evolves with advancements in quantum computing, given their potential to render classical cryptographic solutions ineffective. To keep up with the growing requirements of cybersecurity within the digital defence universe, future improvements should help secure, scale, and enhance the resiliency of the framework to a greater extent.

References

[1] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business horizons, 58(4), 431-440.

[2] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690-1700.

[3] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection Systems. IEEE Access, 7, 41525-41550.

[4] Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169-175.

[5] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-Based Network Intrusion Detection: Techniques, Systems, and Challenges. computers & security, 28(1-2), 18-28.

[6] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: a survey. Journal of Big Data, 2(1), 3.

[7] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in the Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[8] Sun, M., Konstantelos, I., & Strbac, G. (2018). A deep learning-based feature extraction framework for system security assessment. IEEE Transactions on Smart Grid, 10(5), 5007-5020.

[9] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cybersecurity intrusion detection model. Symmetry, 12(5), 754.

[10] Devi, K., Paulraj, D., & Muthusenthil, B. (2020). Deep learning based security model for cloud-based task scheduling. KSII Transactions on Internet and Information Systems (TIIS), 14(9), 3663-3679.

[11] Kaur, P., Sharma, M., & Mittal, M. (2018). A big data and machine learning-based secure healthcare framework. Procedia computer science, 132, 1049-1059.

[12] Kumar, N. (2022). IoT-Enabled Real-Time Data Integration in ERP Systems. International Journal of Scientific Research in Science, Engineering and Technology.

[13] Alsamhi, S. H., Shvetsov, A. V., Kumar, S., et al. (2022). Deep learning for cybersecurity in Industrial Internet of Things: Approaches, challenges, and future directions. IEEE Access, 10, 85792–85812.

[14] Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from a neural network and deep learning perspective. SN Computer Science, 2(3), 154.

[15] Hassan, M. M., Gumaei, A., Aloqaily, M., & Fortino, G. (2019). A deep learning approach for energy-efficient resource management in IoT systems. Future Generation Computer Systems, 104, 38–51.

[16] Odell, L. A., Farrar-Foley, B. T., Kinkel, J. R., Moorthy, R. S., & Schultz, J. A. (2012). Beyond Enterprise Resource Planning (ERP): The Next Generation Enterprise Resource Planning Environment (No. IDAHQP4852).

[17] Hill, C. W. (2007). Transforming the force: a comparative analysis of the Department of Defense's (DoD's) Enterprise Resource Planning (ERP) systems.

[18] Vassilev, V., Donchev, D., & Tonchev, D. (2021). Impact of false positives and false negatives on security risks in transactions under threat.

[19] Bian, J., Al Arafat, A., Xiong, H., Li, J., Li, L., Chen, H., ... & Guo, Z. (2022). Machine learning in real-time Internet of Things (IoT) systems: A survey. IEEE Internet of Things Journal, 9(11), 8364-8386.

[20] Yue, Y., Li, S., Legg, P., & Li, F. (2021). Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey. Security and communication Networks, 2021(1), 8873195.

[21] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. Computers, 12(2), 34.

[22] Thirunagalingam, A. (2023). Improving Automated Data Annotation with Self-Supervised Learning: A Pathway to Robust AI Models Vol. 7, No. 7,(2023) ITAI. International Transactions in Artificial Intelligence, 7(7).