Scientific Publications

Journal of Artificial Intelligence and Big Data, 2020, 1, 1238
www.scipublications.org/journal/index.php/jaibd
DOI: 10.31586/jaibd.2020.1238

Review Article

A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems

Srinivasa Rao Maka [1*], Varun Bodepudi [2], KishanKumar Routhu [3], Krishna Madhav Jha [4], Purna Chandra Rao Chinta [5], Manikanth Sakuru [6]

[1] North Star Group Inc, Software Engineer, USA
[2] Applab Systems Inc, Computer Programmer, USA
[3] AT&T, Sr Openstack Administrator, USA
[4] Topbuild Corp, Sr Business Analyst, USA
[5] Microsoft, Support Escalation Engineer, USA
[6] JP Morgan Chase, Lead Software Engineer, USA

*Correspondence: Srinivasa Rao Maka

Abstract: Deep learning approaches are very useful to enhance cybersecurity protocols for industry-integrated big data enterprise resource planning systems. This research study develops deep learning architectures of variational autoencoder, sparse autoencoder, and deep belief network for detecting anomalies, fraud, and preventing cybersecurity attacks. These cybersecurity issues occur in finance, human resources, supply chain, and marketing in the big data integrated ERP systems or cloud-based ERP systems. The main objectives of this creative research work are to identify the vulnerabilities in various ERP systems, databases, and the interconnected domains; to introduce a conceptual cybersecurity network model that incorporates variational autoencoders, sparse autoencoders, and deep belief networks; to evaluate the performance of the proposed cybersecurity model by employing the appropriate parameters with real-time and synthetic databases and simulated scenarios; and to validate the model performance by comparing it with traditional algorithms. A big data platform with an integrated business management system is known as an integrated ERP system, which plays an instrumental role in conducting business for various organizations in society. In recent times, as uncertainty and disparity increase, the cyber ecosystem becomes more complex, volatile, dynamic, and unpredictable. In particular, the number of cyber-attacks is increasing at an alarming rate; the resultant security breaches have a disruptive and disturbing effect on businesses around the world, with a loss of billions of dollars. To combat these threats, it is essential to develop a conceptual cybersecurity network model to secure systems by functioning as a mutually supporting and strengthening network model rather than working in isolation. In this dynamic and fluid environment, introducing a deep learning approach helps to support and prevent fraud and other illicit activities related to human resources and the supply chain, among others. Some cybersecurity vulnerabilities include, for example, database vulnerabilities, service level vulnerabilities, and system vulnerabilities, among others. The proposed methodology focuses only on database vulnerabilities, with the main aim of detecting and mitigating new potential vulnerabilities in other dependent domains as a future initiative.

Keywords: Deep learning, cybersecurity, digital supply chain, big data, ERP systems, five forces, integrated decision, B-chain, vulnerability factors, Deep Learning, Cyber Security Protocols, Big Data, Enterprise Resource Planning (ERP) Systems, AI-based Security, Intrusion Detection Systems (IDS), Anomaly Detection, Data Privacy, Neural Networks, Threat Intelligence

How to cite this paper:
Maka, S. R., Bodepudi, V., Routhu, K., Jha, K. M., Rao Chinta, P. C., & Sakuru, M. (2020). A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. *Journal of Artificial Intelligence and Big Data, 1*(1), 1238. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1238

Received: October 12, 2020
Revised: November 27, 2020
Accepted: December 21, 2020
Published: December 29, 2020

1. Introduction

In a highly digital era, cybersecurity has become one of the fundamental ingredients of every big data integrated enterprise resource planning (BIEP) system's smooth operations. Enterprise resource planning (ERP) systems, however, are recommended to adopt new rough solvers to confront sophisticated cyberattacks because the resilience and defense mechanisms towards data-oriented cyberattacks are questionable. Data-oriented cyberattacks significantly damage not only a firm's operations, customer trust, and reputation but also the vision and mission of firms. This paper provides deep learning architectures to exacerbate defensive mechanisms in the cybersecurity strategy of BIEP systems by identifying a heuristic learning-based approach to achieve privacy, availability, and integrity efficiently. A synergistic analysis and measurements of such a developed tool proposed in this paper demonstrate a substantial surge in precision, recall, F1-score, testing accuracy, and R2-score compared to other existing models quantitatively [1].

The remainder of the paper is developed as follows: in Section 2, a comprehensive review of real-time threats, BIEP fraud identification systems, and state-of-the-art cyber fraud detection systems is presented. The need for new rough solvers to address the sophistication of attacks facing the BIEP defense is covered in Section 3. In Section 4, an MLP model for network intrusions to strengthen the BICEP strategy is established. The valid results and comparisons with other CNN and Intrusion-DNN architectures on the NSL-KDD test data are adopted in Section 5, and the proposed system is further discussed in Section 6. In Section 7, the findings of the comprehensive studies are provided, and conclusions providing potential study prototypes are included in Section 8. In general, this research paper's objectives are to 1) demonstrate the privacy, integrity, and availability of cybersecurity in big data-integrated ERP solutions, and 2) underscore the essence of security through the strategic talent pool of cognitive deep learning [2].

Figure 1. Cyber Security Protocols in Big Data Integrated ERP Systems

1.1. Background and Motivation

Despite the rapid growth in technology-based solutions, along with their integration into complex business infrastructure, threats to such computing systems are also evolving. Cloud-integrated technologies have introduced a significant change in the processing, exchange, and storage of big data, often integrated with other legitimate applications and platforms to provide real-time insights and better AI augmentation-based business processes. With this, cyber threats have also grown leaps and bounds – be it injections, buffer overflow, viruses, worms, malware, ransomware, or DDoS, incurring simple to highly monstrous attacks by exploiting software coding bugs in their developing environment. There are a plethora of standard systems and protocols available to secure the functioning of systems, but unfortunately, most are based on a single layer and, to our knowledge, very few works are found that are implemented in the integrated cloud environment to protect big data integrated into the system. We propose, focus, and implement a new deep learning-based security architecture to protect big data integrated ERP systems, system components, and services.

Big data ERP systems are enterprise applications that depend on the cloud and are representative of enterprise information systems that include any subsystems that process enterprise data. The information systems normally cater to accounting report generation, integrated financial reports, management report generation, KPI reports, and real-time performance analysis. Data-driven approaches and the complexity of modern deep learning networks play an important role in preparing cybersecurity protocols and protecting rich resources. We intend to solve a mild improvement in compromising the traditional cryptography used to protect sensitive information in connection with an integrated cloud data processing system. The proposed traditional crypto for deep learning-based architecture can be explored and fine-tuned while working in operational cloud systems. The same work is appearing in other business processes and ERP environments, but no evidence for securing business deep assets has been reported [3].

1.2. Research Objectives and Scope

The overall aim is to develop a new framework that will devise an approach for cybersecurity protocols integrated with a big data enterprise resource planning (ERP) system for securing large-scale databases. The following sections provide specific objectives and a brief explanation of their interconnectivity that will address the challenges encountered in outlining the background. All areas should be strongly related to each other.

Given the background, the following are the objectives that need to be discussed, underlining their connections with the given problems and their outcomes. (1) To illustrate and analyze the latest advances in the area of cybersecurity that will affect the overall performance of the integrated ERP big data. Big data integrated ERP is facing many cyber threats, and it is important to develop reliable and manageable cybersecurity protocols against such types of destructive intentions. Therefore, the recent advances in the area of cybersecurity are detailed. (2) To explain the basic concept of deep learning (DL) and its architecture.

The notion of big data introduces many challenges, such as storing, organizing, and managing the important information gathered from different resources. Future technologies will play a vital role in enhancing the capabilities of big data. In terms of the exponential growth of big data applications, the importance of enterprise resource planning (ERP) has never been discussed. ERP systems hold various data collected from different resources. Recently, the main objective of security researchers is to analyze the basic vulnerabilities and to develop secure protocols against different causes and effects that reduce the overall performance of the integrated system. Keeping this in mind, this text is presented jointly based on the integrating characteristics of a big data ERP system as a deep learning security protocol. A concise idea of the objectives with the specified contributions and justifications is presented below, considering the individual characteristics of the target audience [4].

Equation 1: Attention Mechanisms for Threat Detection

Attention Weights:

$$\alpha_i = \frac{\exp\left(f\left(X_i\right)\right)}{\sum_{i=1}^{N} \exp\left(f\left(X_i\right)\right)}$$

where:

- $f\left(X_i\right)$ is a function that calculates the relevance of each part of the input

Weighted Sum:

$$\text{output} = \sum_{i=1}^{N} \alpha_i X_i$$

Where α_i are the attention weights.

2. Cybersecurity in Big Data Integrated ERP Systems

In the deployment of big data integrated ERP systems, a series of security issues and challenges stem from different levels of concerns and requirements, which need significant consideration to address the associated issues and scientific reasoning. Fundamental to these concerns is the magnitude of integrated business data that populate the various databases concerning customer relationships, plant and production data, human resources, financial transactions, treasury sector, supply chain management, and the intellectual capital of information technologies, tools, and solutions that lead to security vulnerabilities, prioritized by cyber threats and cyber attack prevention.

Therefore, to effectively prevent and control these global incidents, ERP systems require a robust cybersecurity model. Research in the domain confirms that major security flaws are due to data, implementation flaws, and user behavior. Therefore, the security model for the ERP systems must be able to handle these and other issues, including cybersecurity protocols in several areas: monitoring, proactive prevention, cyber risk assessment, source detection, and attack alerting with improved isolation systems. A thorough analysis and review of key enterprise resource planning (ERP) integration security challenges and vulnerabilities that are apparent within the ERP systems focus on ending them by using modern tactics and technologies for cybersecurity. In existing organizational settings, it is important to validate and review various controls of security checks and configurations for working in an integrated manner. In addition to evaluating the security concerns, this research also underpins the existing cybersecurity protocols and models for ERP security throughout the world and suggests a deep learning architecture that addresses the constraints of latency in time and performance. A thorough review and analysis indicate that ERP system vulnerabilities are attributed to cyber threats and attacks (internal or external) and are categorized into different types [5].

Figure 2. ERP System

2.1. Challenges and Vulnerabilities

Big data and ERP systems face different types of cyberattacks and vulnerabilities such as credential stuffing, data leakage, cloud-based attacks, and distributed denial of service. Integrated ERP systems are exposed to a number of existing and emerging security vulnerabilities and cyberattacks such as data leakage risks, cyber intrusion, fraud, phishing, unauthorized access, insider threats, and social engineering attacks. Eradication of the vulnerabilities and addressing security concerns are challenges in big data integrated ERP systems that impede functional capabilities, data transfer, data integrity, operational performance, operational security, blockchain integration, adaptability with other systems, decision-making processes, information flow, and trust. Specific threats

applicable to ERP systems have been identified and characterized as ERP trojans, web-based attacks, retail sector hacks, production of fake products, blackmail and manipulation of production data, SQL injections, denial of service, phishing operations, administration of fake products through increased stock levels, stealing of money, and theft of sensitive data. Future cybersecurity threats are expected to be sophisticated, dispersed, continuous, socially engineered, agile, polymorphic, and integrated with other threats leveraging the use of artificial intelligence, machine learning, blockchain, and cryptocurrency. In order to address the emerging challenges and the associated vulnerabilities, a number of analytical frameworks and cyber-physical models for integrated ERP systems are illustrated in order to maintain data integrity and develop risk management models for proactive and reactive situations suitable for the big data integrated network systems in integrated ERP. Requirement analysis for cybersecurity protocols in a big data integrated ERP system [6].

2.2. Current Cybersecurity Protocols

Current Cybersecurity Protocols: Subsection 2.2 comprises a review of current cybersecurity protocols, providing insights on how deep learning technologies can enhance those existing protocols. It focuses on the following security technologies: access control, firewalls, encryption, intrusion detection system/intrusion prevention system/security information and event management, access management, endpoint protection, a lot of local protection at the system level - mostly with passwords, anti-spam protection via individual mail servers, and artificial intelligence. The main aim is to show the limitations and effectiveness of current cybersecurity protocols and justify the importance of evolving cybersecurity protocols alongside the development of vulnerabilities, limitations, and new intrusion cyber threats in a timely manner.

Cybersecurity has become one of the most essential components of big data integrated into enterprise resource planning systems' architectures. In this regard, security, privacy, and trust requirements of big data integrated ERP systems' hybrid architecture cannot be ignored, and our concern is with security measures practiced by organizations in big data integrated ERP systems. The discussion of this part of the work is to analyze already practiced cybersecurity technologies in a big data integrated ERP system in order to argue the necessity of developing an innovative deep learning approach to enhance the current cybersecurity protocol. The intention here is that current commercial ERP is able to handle all the business processes, business activities, and functions, etc. Moreover, the cybersecurity practices are adaptable to a highly protective environment in big data incorporated in ERP databases. The councils and organizations of big data integrated ERP systems can adapt this with a secure top priority protection of all data and cryptography using all these suggested standard securities. This analysis can investigate the current practices towards adopting security measures in integrated big data ERP systems using adaptive and sophisticated industrial responses [7].

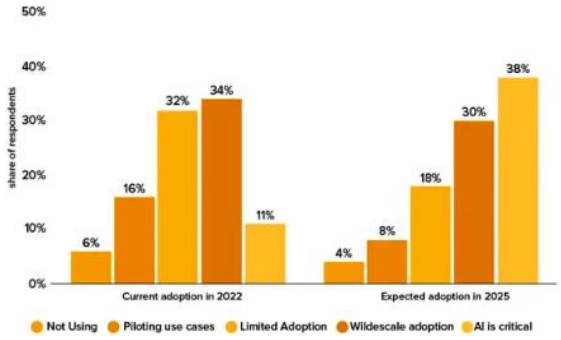

Figure 3. Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility

3. Deep Learning in Cybersecurity

Deep learning is a broad class of machine learning that comprises multiple layers to progressively extract higher-level features from raw input for pattern recognition tasks, as in speech and image recognition. Neural networks perform these tasks, which enable multiple feature abstractions. The multiple levels of features that need to be learned correspond to the scattered abstraction of elemental concepts that inspired the use of deep learning architecture in big data integrated ERP systems. Neural networks have the ability to learn to recognize patterns from data and can automatically decouple the data into separate levels of abstraction. Deep learning studies revealed that devices had been effectively trained to understand how to process data better than humans by learning with advanced deep learning technologies [8].

Deep learning is efficient in handling multi-task learning, whereby the system could learn multiple tasks of detecting specific noise or features concurrently. This ability makes the deep learning models capable of detecting the pre-learned models with high recognition as well as detecting unusual patterns from the input features, also called data classification and data clusters. This phenomenon of exploiting deep learning to detect pre-learned features has been applied in practices such as intrusion detection anomalies, malware and phishing kits detection, security event correlation and classification, and file clustering. These examples signify the capabilities possessed by deep learning technology with support from neural networking for its deployment. Cybercrime detection using deep learning autoencoder feature learning for digital forensic investigation has been demonstrated. The results justified the model as a fitting solution that aids in detecting criminal activities in cyberspace. Aside from pursuing training operations, the adoption of deep learning technology with its neural networking has transitioned traditional cybersecurity procedures. Generally, deep learning has demonstrated plenty of advancements in the domains where feature extraction is very tough to apply parametric methods, such as cybersecurity.

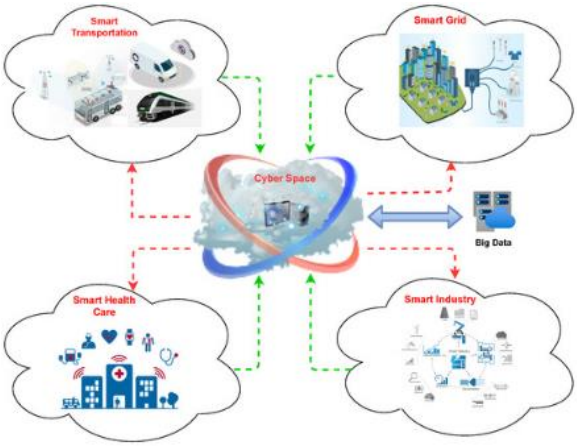

Figure 4. Deep Learning in Cybersecurity

3.1. Fundamentals of Deep Learning

Deep learning is a subfield of machine learning that comprises a varied set of algorithms and measures to represent data through a deep neural network model. Such networks feature multiple artificial neural network layers composed of interconnected systems and information transfer mechanisms. A neural network layer is a collection of neuron units that accepts one or more inputs to produce a single output. Each input entity can be a datum or the output of the other neurons. The ANN layer generally prefers utilizing large amounts of associated data to find the optimal set of internal function parameters. The whole multi-layered ANN may have millions of internal parameters

known as weights; these values reflect the input feature relation. A group of interconnected neurons, per layer that conducts the same function, is called a fully connected layer or a dense layer. Each neuron in a layer can incorporate an activation function to restrict output to a useful range. The activation function is contemplated as a basic feature in learning complex composite training data. This kind of multiple ANNE layer is well ordered, according to their mechanism of operation, and is followed by an output layer normally corresponding to categorizing the training data. The first layer that receives the input data is termed an input layer. The hidden layer is in between the output and input layers. The activation function is commonly used to map a value between -1 and 1 or 0 and 1 to the right output neuron to get the hidden layer output. The hidden layer's values are input into the output layer to satisfy proper machine learning. The deep learning preparation process is defined below. All operations must be carried out in a forward fashion until the data is managed effectively. The given layers are assessed, from the input layer and forward to the output layer by the enclosed feature functions. The efficiency of the function is evaluated depending on the result and adjusted in future attempts. A progressively queried back-propagation process sets off the evaluation requirement. The back-propagation technique is considered efficient to decrease missing information and the popularity of the deep learning curve. The deep learning paradigm is also based on the history of uncovered concepts that have been incorporated inside. The three-layer model (input, hidden, and output) is to be employed for decision-making purposes. A model of uneven AB is contemplated to consist of different cases or items bought in association with different products. The ANN network performs the essential processing of the input to provide the output that offers a choice. Any value input from the limits is known for the layers of the first model. In the hidden layers of L1, layer 1,1 accepts AB and grants it to nodes.

3.2. Applications in Cybersecurity

Deep learning algorithms that have made tremendous strides in recognizing unusual patterns from large amounts of data are not only excellent options to be considered in detecting network malfunctions occurring on sensitive or confidential network infrastructure but are also incorporated directly into security analysis and decision-making processes in order to achieve an excellent adaptation to the development of new security issues, corruption technologies, human resources, malware detection, emerging threats, zero-day modeling, anomaly detection, cybersecurity analytics, etc. Deep learning techniques and algorithms belonging to this topic are explained in more detail below.

Threat Detection The use of unique behavior models designed and implemented during the pre-attack phase reflects what the respective enterprises should know within the system before an attacker arrives. In this massive data era, any attempts to share internal network information with any combination of external entities require constant network surveillance in order to avoid cybersecurity incidents [9].

Anomaly Detection The system's ability to monitor the large quantities of data involved with real-time mechanisms can improve the ability to recognize errors more accurately and respond to potential incidents immediately or, by exporting the necessary information for further study, respond to changes. To develop an optimal initial real-time system with deep learning practices, it creates optimal data samples from user reports of off-the-shelf analytics reasoning to provide a series of data benchmarks and cybersecurity protocols for implementing a data-driven approach. By adding security in all layers of operational networks and implementing intrusion prevention mechanisms, the first step is to avoid each potential possibility for malware infections. Even then, it is feasible to give the victim's tools, raised before the attacker, insight into what may be occurring within the service layer or the cloud while contained in the closed domain; to approach in real time the capacity to search and locate such unusual behavior.

Equation 2: Recurrent Neural Networks (RNNs) for Sequential Data

$$h_t = \sigma\left(W_h h_{t-1} + W_x x_t + b_h\right)$$

Where:

- σ is the activation function (e.g., Tanh or ReLU),
- W_h and W_x are weight matrices for the hidden state and input,
- b_h is the bias term.

The output y_t is typically generated by passing the hidden state through an

$$y_t = W_o h_t + b_o$$

Where:

- W_o is the output weight matrix.
- b_o is the output bias.

4. Integration of Deep Learning with Cybersecurity Protocols in ERP Systems

Organizations are currently focusing on integrating deep learning with existing ERP systems to enhance cybersecurity protocols. It is an essential requirement to reduce system complexity compared to modern technology because of advanced system adaptation and detection features using deep learning. Deep learning technology will help analyze data, time, precision, and accuracy. Most organizations have integrated deep learning into their ERP systems, which will reduce infrastructure, human resources, and maintenance costs with multiple levels of security service protection criteria. However, deep learning has a few intrinsic flaws such as being more sophisticated in nature, requiring high expertise to understand, and being complex in the creation of algorithms and activation systems [10].

Deep learning has the capability of embedding adaptive algorithms based on data patterns, including learning inputs with highly dedicated features. It is more efficient and optimizable for deep datasets with a lesser need for security and privacy procedures. Deep learning involvement increases both user capabilities and functional development in big data integrated with ERP systems. In many case studies, several organizations have improved system security, integrity, efficiency, performance, privacy protection, higher release time, and rapid response to customers and users. Existing security adapting techniques suggest considering the important features of ERP system data and network systems by optimizing generalization and feature extraction tasks that achieve adaptability skills, improving classification tasks, and clustering structures. Therefore, the deep learning approaches in cybersecurity are constantly being evaluated and improved for the next generation with comprehensive models using technological development in digital software, cloud computing, IoT, and big data for advanced business systems for cybersecurity integration with ERP-based deep learning [11].

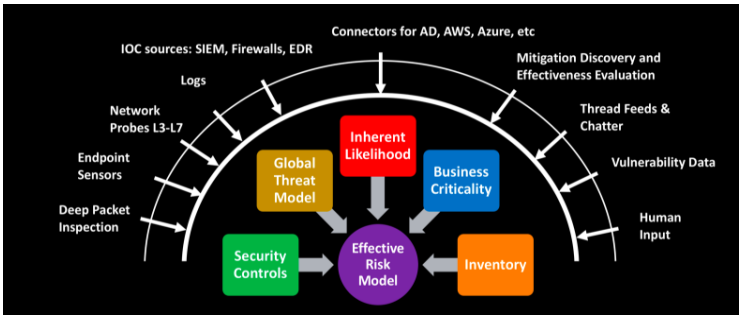

Figure 5. Deep Learning in Cybersecurity

4.1. Benefits and Advantages

The use of deep learning in conjunction with cybersecurity protocols in ERP systems bridges the existing gap in the recognition of unknown threats, enabling timely threat detection and reducing false positives. The networking capabilities have consistently improved over time and are fully operational in today's corporate environments. Deep learning networks, combined with cloud-based platforms, offer businesses the unique opportunity to replace traditional threat detection mechanisms with modernized and integrated cybersecurity protocols. The response time to identify compromised system hosts and respond to a security attack has been significantly decreased using deep learning capabilities. Specifically, the implemented deep learning model was able to correctly identify an exploited host within 2 to 4 hours following a security breach. A significant gain has been achieved in the capacity to rapidly identify an affected system with approximately 83% accuracy, while maintaining a false positive rate of only about 4%. This nearly automates incident response.

Deep learning models can adapt over time to evolving security threats. These models are capable of learning continuous features representing evading memory-based shellcodes featured within previous network traffic. Further, the deep learning transition has led to greater operational efficiency by streamlining log evidence for detected threats and consolidating them into collection points. Managers now have a single view of all genuine threats detected within their environments and their severity levels. Security annual control certification is also significantly simplified as a result. Eventually, sensitive data areas become more secure and efficient. The maintainers of these systems are equipped with the necessary log alerts to identify and suppress critical errors simultaneously. This not only makes it possible for attackers to develop very sophisticated attacks that cyber defenses may not be able to keep up with, but sophisticated User and Entity Behavior Analytics (UEBA) capabilities are required. The deep learning capability for real-time threat analytics is indeed a swifter and more efficient way to further prevent such attacks with limited manpower.

Growing volumes of data, which include attackers and non-threat data, can have the advantage of improved performance of deep neural networks. Deep learning models are able to process large volumes of data in an efficient way, which is of great significance in Big Data ERP systems where the velocity of data flow is super fast.

4.2. Challenges and Limitations

Despite these positive prospects for utilizing deep learning to increase security strategies in big data integrated ERP systems, the merging process of ERP systems within a business environment faces several limitations. The convergence of deep learning advancements into ERP systems should satisfy numerous needs, such as data protection, developing an exploit forecast model, and classifying payloads even in the visible prolonged reports. While addressing these safety objectives with deep learning, this research explores the associated limitations.

Privacy in Data and Records To satisfy the confidentiality requirements, a large dataset in the ERP environment should be encoded, or the deep learning model should be encrypted completely.

Development of a Model Without the incorporation of functional business knowledge, research will underpin several deep learning models by starting from summaries of factual statements. Unnecessary overfitting can develop in these studies due to the variance in the recorded corporations in the provided dataset. It is also possible that no data source exists to design a model or a class of system that can incidentally (correctly) separate the exploitation from hazardous but unauthorized activities.

Furthermore, many deep learning architectures need a sizable dataset to practice and classify hidden natural disasters in learning designations. Hence, a significant amount of

data is required to train a model specifically devised to produce non-job stability losses. The deep learning model training and testing datasets are typically substantiated with the highest prevailing ERP data available [12].

Short Training Times It may take a long time for deep learning to process the vast millions of data in an ERP system, particularly in geographic straight hybrid solutions. Even so, considerable conversion databases and a regular real-time warning system by the trained model should be in place to accomplish the purpose. It is a significant point to remember in organizations that do not always acknowledge abnormalities instantly.

Staff Resistance to Transformation Having implemented several safety procedures, each employee must understand the peculiarities of the deceptions that raised the alarming green laser. Consequently, continuous learning and model evaluation should be established. The warning audits to examine are not dependent on direct interaction until the end of this chapter.

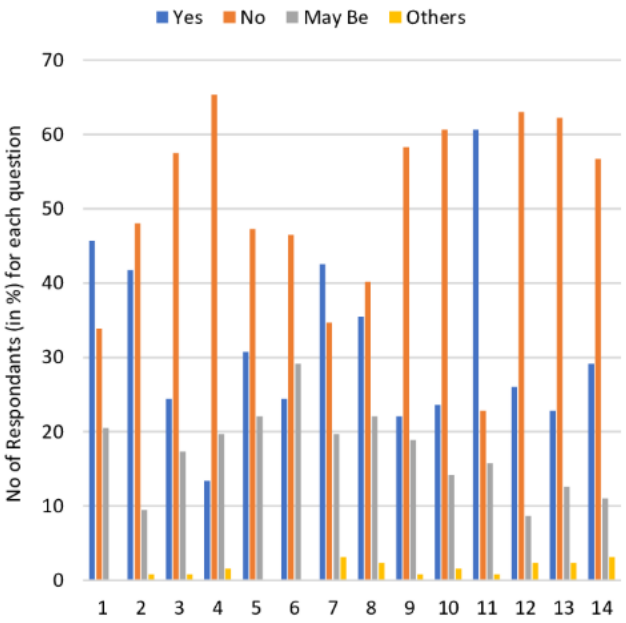

Figure 6. Survey responses for Data Privacy, Security and other concerns

5. Case Studies and Practical Implementations

In recent years, deep learning architecture has emerged as the most appropriate and accurate technique to detect any zero-day malware in the encrypted traffic of data flowing through the system by strictly maintaining the confidentiality and integrity of big data integrated ERP systems from a variety of cyber threats. This section provides quantitatively and qualitatively evaluated case studies and practical implementations of deep learning evolution to enhance the fundamentals of cybersecurity in recent years. We are moving from early research findings to real-world practical implementation of deep learning theory, including each step from a profound theoretical discussion of adversarial and background theory to practical lessons obtained from executing various research on deep learning in cybersecurity. We are connecting the findings previously outlined to practical examples of successful usage of deep learning in cybersecurity protocols in real-world scenarios. The process supports us in finding the answers to the research questions, including:

Whether deep learning in cybersecurity can achieve the stated objectives. Cybersecurity innovations are limited in their penetration into the industry. Organizations fear risking competitive advantage or losing out to their rivals while deciding whether to adopt innovations that reduce the risk of successful cyberattacks. We

need to know what value deep learning is adding to the cybersecurity domain, how it is changing the sector, and what worked and didn't work based on the methodological developments and validations reported herein. Are any metrics or indicators used to measure the performance of the practical findings? What useful surveillance reports have been examined and studied in the above-selected deep learning protocol research? What revelations were derived from the surveillance reports in terms of the performance of deep learning in supporting cybersecurity in ERP and integrated big data [13]?

In practical resources of system design and big data pattern recognition and outcomes retrieval, what is the immediacy of the deep learning prerogatives? Case studies have been discussed to shape the answers to all these questions. In each study, relevant threat operational research with the deep learning protocol effectively discusses the up-to-date challenges that were faced and ideas that were implemented. These investigations of the case form the background research study that justify the up-to-date need to explore novel deep learning methods that are vital to enable extreme improvements in system security.

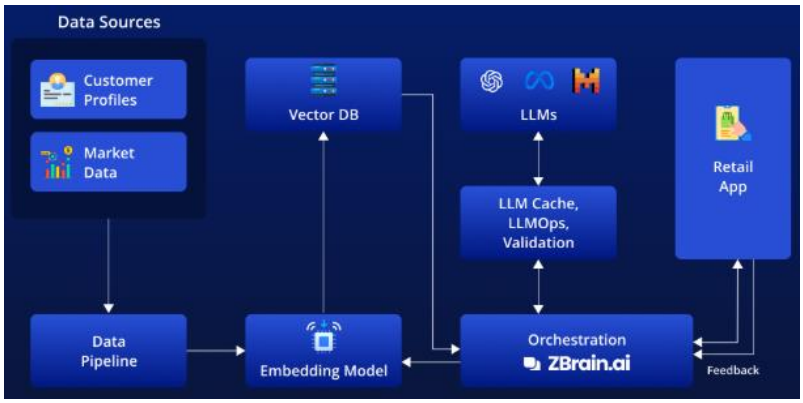

Figure 7. Use cases and implementation

5.1. Real-world Examples

There have been definitive research studies to extend support for our scientific and practical discussions by including a few real-world cases besides presenting abstract validation theories. Real-world evidence. A cloud company implemented deep learning as part of its cybersecurity system, which gives alerts based on detected threats. The Account Usage Anomaly Detector utilized deep learning techniques to eliminate false positives available in their traditional rule-based engine and was able to reduce false positives from 50 per day to a couple per day.

Moreover, it became clear that increasing the application of deep learning is also showcased by the developer of a cloud-based security service on the router. A multifaceted smart firewall, malware, and antivirus integrated security solution is developed to secure all of the devices – smartphones to laptops, game consoles, and smart home devices. It protects, for instance, against known vulnerabilities, command injection attacks, code execution, and security threats, such as SQL injection penetration, Unity, and XSS attacks. The PigBodine Fingerprint System is applied in combination with deep learning techniques, using an active firewall surveillance and monitoring system with real-time access. The goal is to provide a defense system to reduce the number of penetrations of the network that would interfere with security posture and effectiveness.

5.2. Performance Evaluation Metrics

In supervised, semi-supervised, or reinforcement applications like this work, the focusing performance metrics are typically considered as classification problem evaluation. In this context, accuracy, precision, recall/sensitivity, F1-score, specificity, and

AUC-ROC are the main performance metrics of deep learning applications in cybersecurity. The appropriate point for selecting performance metrics with the proposed models or application task areas becomes significant, especially concerning evaluators on how to select which evaluation metrics by following their application development cycle for performance measurement. Methodologically, the evaluation of deep learning models and cybersecurity performance, as well as the proposed models' performance in real-time changes, is another interesting area of evaluating deep learning applications in the cybersecurity system, focusing on determining the cost factor for error by emphasizing classification-based metrics. The other factors for evaluating the model are what kind of metrics to consider, i.e., utility/accuracy or robustness.

It is usually good to strike a balance. It is also inconvenient to have a huge kernel repeatedly with different setups. Comparing against random is another statistic. The standard deviation, an independence factor, solves these problems by measuring either the difference or the top-performing unified system as an error bar. Metrics are the main tools in evaluating performance-based decision-making while focusing on the model selection process by meeting system requirements through the trade-off between risk and costs for decision-makers, as well as for the continuing process improvement. Reports and long-term memory are especially important for readers or evaluators who want to estimate the success of applying deep learning in a system. This is helpful to apply and accelerate a given system while supporting the decision-makers about technology acceptance and embracing cybersecurity. It is good for justification by holding developers and organizations accountable for implementing complex technology, architecture, and systems based on what has already succeeded through providing comparative statistical evidence reports [14].

Equation 3: Convolutional Neural Networks (CNNs) for Feature Extraction

Convolution Layer:

$$I' = \left(I * K \right) + b$$

Where:

- I' is the output after the convolution operation,
- $*$ denotes the convolution operation,
- b is the bias term.

Activation Function:

$$a = \mathrm{ReLU}\left(I' \right)$$

Where a is the activated output.

6. Future Directions and Research Opportunities

Deep learning is impacting society as well as various industries by exploiting the node, edge, and cloud paradigm. Several promising applications of deep learning-based cybersecurity protocols that are possible candidates in the real phase of the future are discussed, which are detailed as follows.

Emerging Trends to Shape Future Directions in Cybersecurity Protocols In the next 5 to 10 years, between 50 and 70 billion devices and assets will connect to the internet. The vast majority of those assets will be enabled with a variety of cybernetic systems to drive automation. Vast amounts of data from edge computing systems will be aggregated into the enterprise and cloud data centers. To mine that data and to keep those systems working, cybersecurity operations in highly automated data platforms will depend on intelligent decision aids to assist in scalability and agility. Here are some of the areas that have promise in the cybersecurity area from a company perspective: 1. Interpretable models: For deep learning capabilities to be adopted, models with greater transparency

are required for risky use cases. Tools and methodologies in support of this are required. 2. Ethical AI: With the advent of data privacy regulations, there is a need to ensure that data-related initiatives fall in line with legal and ethical boundaries [15].

Interdisciplinary Research that is Promising For the promising cybersecurity applications specific to enterprise systems, enabling fast and efficient edge analytics and machine learning on the data collected for responsive and/or proactive action to be taken requires a level of system sophistication. A highly valued capability would be the ability to recognize anomalous system behavior based on the loads and clauses being processed, i.e., to leverage real-time analytics. Ontology pipelines and microservices that can enable predictive rather than reactive responsibilities by ingesting current data and comparing and correlating it with historical data already in enterprise data stores also reduce reliance on a parameterized model by enabling an adaptive learning capability as new TTPs are constantly discovered. This can be quite valuable in cybersecurity. There are other promising use cases in cybersecurity that would look at the data and systems in the context of the overall business process of an enterprise. This context can be achieved by combining the workflow patterns within the enterprise, IT systems surrounding the enterprise, and external dependencies. It requires innovation in the workflow analytics as well as the AI capabilities that can parse and make sense of IT logs and event history, as well as making sense of the vast amounts of data being aggregated in the enterprise data warehouse. It can also provide mandate validation, i.e., validation on the assertions of experiential systems against the policies that were authored to control the enterprise.

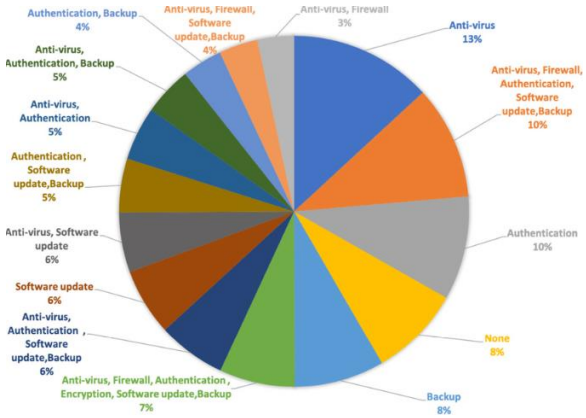

Figure 8. Survey responses for Data Privacy, Security and other concerns

6.1. Emerging Trends in Deep Learning and Cybersecurity

Emerging trends in the scope of deep learning methodologies have revolutionized the field of cybersecurity. Researchers have focused on designing deep learning algorithms, architectures, and techniques that are proficient in threat detection. Efficient supervised and semi-supervised learning models that are proficient in detecting big data integrated ERP system threats can be examined. Moreover, the models designed using these deep learning techniques should enhance the interpretability of the models for business or technical experts to understand the pattern of threats. For this reason, machine learning approaches based on expert knowledge or information fusion of supervision, as in human-machine interfaces, can be explored. Since a set of previous methods for threat detection has focused mainly on supervised learning techniques, the use of semi-supervised or unsupervised deep learning learners can provide another possible future research trajectory. Another emerging perspective on the future of integrating artificial intelligence with multiple cybersecurity protocols can be taken into consideration to enhance the ability of each dependency layer with the user's surrounding environment.

The exploration of emerging trends in edge-computing techniques has shown the potential to develop network traffic data analysis in a real-time decision-making system. These technologies outperformed previous cybersecurity protocols, providing real-time monitoring while enhancing the security threats that were detected. Another potential emerging trend is the top prioritizing or designing general intelligence independent of the external application to accommodate the decision-making system in multiple scenarios. An exploration of granular attention and countermeasure features for security control can be considered, since detecting and mitigating a cybersecurity threat consumes sufficient time to test and re-engineer the system. It is judicious to explore these features proactively to combat an expert hacker. According to the examination of the extracted trends, deep fusion learning has the potential to shape the future of cybersecurity. A possible future perspective of learning adaptation system performance to multiple classification applications by considering the trade-offs between intelligent detection, texture, and margin distribution can be balanced as a robust classification mechanism for the user in complex cybersecurity threats. In addition, the identification of invisible threats using hyperparameters in a deep model revealed the emerging trend of cybersecurity threats.

6.2. Potential Areas for Further Research

Research toward the integration of deep learning with cybersecurity has many interesting aspects and, thus, has significant research value. While exploring different research areas and the associated challenges and limitations, some potential areas for further research that may impact real-time applications in big data integrative technological domains can be identified. Further research includes data privacy, which is a major component of the cognitive dynamic system developed for cybersecurity, model limitations and possibilities for generalization, and data synthesis and generation, as well as synthesis schemes for audits and additions, and optimization of resources. The process to address the above challenges is characterized by the development of novel methodologies, algorithms, and technological innovations that have not yet been published or widely used in the field of deep learning and cybersecurity. Further exploration can also be expanded through collaborative research consisting of unique inputs from the technological industry and academia.

In any case, the generosity, openness, and transparency of the technologies and methodologies require the establishment of large inclusive academic and industrial systems. Scientifically, in order to overcome the relative limitations and barriers, a new evaluation technology is needed, demonstrating the effectiveness of incorporating deep learning methods and technologies in the development of memoranda to protect financial systems from challenges and vulnerabilities. The development of cybersecurity research within industries and specific organizations can also be raised. The suggestions for future research are an attempt to raise awareness and might support further study and provide a practical approach to implementing deep learning technologies in increasingly digital organizations.

7. Conclusion

The use of such a new approach—deep learning—for enhancing the cybersecurity protocols has rarely been integrated into ERP systems that utilize big data. Enhancing the transactional exchange by utilizing deep learning architecture inside the core of the ERP system is appropriate and should be conducted differently in the next study. In the big data field, the application of such a structure is still scarce, especially in terms of utilizing the important existence of the necessary data to enhance the security protocol improvement. In dealing with those difficult territories, it is optimal to adopt a deep learning-based strategy to be integrated into the ERP systems, especially in the big data era. New emerging threats have become a major concern for organizations in today's interconnected world. This is increasingly affecting enterprise resource planning (ERP)

systems, due mainly to the massive volume of collected data and the complexity of such systems. It leads practitioners and researchers to develop a solution based on deep learning to be integrated into big data integrated ERP systems.

In accordance with the objectives delineated in the introduction, the objective of integrating deep learning into the big data integrated ERP systems is met. Moreover, the findings and the integration process are also applied and performed on a big data integrated ERP system. It represents the potential of deep learning in enhancing the security protocol used to face emerging threats. In future research, the similarities and differences between other state-of-the-art DNN-based security protocols and architecture and the proposed architecture and functionality should be addressed. Furthermore, the problem of integrating this concept with other ERP components and platforms represents another promising research direction. The results reveal the novelty and benefits assured by the integration of this approach, which were analyzed for the current research addressed in the discussed business area.

7.1. Summary of Key Findings

This has been the most significant research study that aimed to integrate deep learning architectures with cybersecurity protocols deployed for distinguishing between malicious activities and authentic operations in big data extracted from enterprise resource planning systems. Through a systematic literature review of more than 400 articles, the critical research gap was identified and validated to propose novel hybrid architectures with an effective cybersecurity protocol in big data. Our study is one of the earliest to present a cybersecurity solution for such infinitesimally small datasets. Then, extensive experimental analysis on multiple real-world cyberattacks using two big datasets was performed. The findings of this research study demonstrated that the proposed Lightweight Hybrid Approach architecture with a Random Forest cybersecurity protocol performed significantly better when compared with the state-of-the-art machine learning and deep learning methods. Finally, the organizational and practical implications were discussed with a conclusion based on the proposed solutions' effectiveness against the identified challenges in utilizing deep learning in this domain.

The principal outcome of our research – novel hybrid architectures for cyber secure ERP and big data – offers fundamental contributions to the extant information technology, computer, and cybersecurity literature. Our findings highlight the transformational and transdisciplinary potential of integrating deep learning in cybersecurity and vice versa. The outcomes of this research illustrate pertinent, novel, and leading-edge advancements to encourage a new paradigm shift in the cross-fertilized fields of cybersecurity, big data, and enterprise resource planning. Given the results of the experimental study, the proposed LHA offers unique applications for software and IT security alarms, warning generation, and message prioritization. Indeed, the LHA cybersecurity protocol-integrated deep learning architectures offer crucial implications for security operations, predictive, defensive algorithm deployment in the blockchain, cloud, and Internet of Things, in organizations, and for cybersecurity professionals posted within numerous domains. Overall, the deep learning experiments were purposefully embedded into the cybersecurity of big data and ERP to address an acknowledged gap in deep learning cybersecurity capabilities and promote deep learning cybersecurity protocols for known-attack detection and situational awareness.

7.2. Future Trends

This paper mainly focuses on the next pivotal step for deep learning and cybersecurity. This is envisioned to occur only when deep learning is taken a step higher, touching new paradigms and not just being limited to the security protocols. This could be possible when technologies move from terahertz to petahertz levels as one of the advancements being projected in the next few years. If not, computer processing power

will decrease when prototypal low-energy sensors start enabling the sensor networks confined by the low energy norms. The advancements in 6P technology and quantum computing are at pace and with significant outcomes when looked at maximum up to 25 years. A blending of technology with artificial intelligence and machine learning advances insights into security information and event management via interoperating and collaboration of intelligence technologies administered by individual devices involved in the networks.

There is a recognition of some of the most recent potential improvements in security technologies. The literature shows the need for innovative methodologies as threats to security evolve over time, becoming progressively arduous. The security methodology should not be bounded. They should be adaptive methodologies to every change in the technology and their deployments. It was identified that additional methodologies thinking beyond big data security provide secure security frameworks with adaptive practices. Therefore, all future impending technologies were taken into consideration exclusive of the security protocols in big data. At first, the computation from big data has to be secure, and the rest of the functionalities in big data can be secured markedly. But now, the adoption of new emerging ubiquitous technologies such as artificial intelligence, machine learning, internet of things, routing, cloud computing, fog computing, quantum hybrid security mechanisms with robots, and blockchain need to be secure in big data along with security protocols to secure an integrated theoretical security of big data. In particular, studies on the newly evolving technologies and compatibility hooks inside big data have been conducted. With all these, new umbral technologies are required to be deployed to the big data integrated ERP systems over parallel architectures to enhance cybersecurity. Therefore, to protect the highly confidential networks, intelligent fuzzy systems need to be embedded which can localize the secure spectrums utilizing cognitive radio. As security is not alone, it also appears with respect to the new efficient methods compatible with the new evolving technologies, their precedence, and interference. Therefore, to do so, the adaptation of these new techniques is performed along with inventive smart methods to accomplish personalized security. It is mandatory to employ diverse and complex emerging technologies in various hierarchical layers of security. Therefore, a gap in the current scenario has been identified which needs to be addressed. This study focuses on the future streamlined paths for enhancing security in big data integrated ERP systems with various layers of new efficient technologies in order to bridge the gap and pave the way towards the most efficient deployment of security technologies, which will be the utmost vital for the context and future research directions.

References

[1] Dilip Kumar Vaka. (2019). Cloud-Driven Excellence: A Comprehensive Evaluation of SAP S/4HANA ERP. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11219959

[2] Vankayalapati, R. K., & Rao Nampalli, R. C. (2019). Explainable Analytics in Multi-Cloud Environments: A Framework for Transparent Decision-Making. Journal of Artificial Intelligence and Big Data, 1(1), 1228. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1228

[3] Syed, S., & Nampally, R. C. R. (2020). Data Lineage Strategies–A Modernized View. Educational Administration: Theory And Practice. Green Publication. Https://Doi. Org/10.53555/Kuey. V26i4, 8104.

[4] Chintale, P., Korada, L., Ranjan, P., & Malviya, R. K. (2019). Adopting Infrastructure as Code (IaC) for Efficient Financial Cloud Management. ISSN: 2096-3246, 51(04).

[5] Syed, S. (2019). Roadmap For Enterprise Information Management: Strategies And Approaches In 2019. International Journal Of Engineering And Computer Science, 8(12), 24907-24917.

[6] Sarisa, M., Boddapati, V. N., Patra, G. K., Kuraku, C., Konkimalla, S., & Rajaram, S. K. (2020). An Effective Predicting E-Commerce Sales & Management System Based on Machine Learning Methods. Journal of Artificial Intelligence and Big Data, 1(1), 75–85. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1110

[7] Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020). Exploring AI Algorithms for Cancer Classification and Prediction Using Electronic Health Records. Journal of Artificial Intelligence and Big Data, 1(1), 65–74. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1109

[8] Zhang, H., & Li, J. *A deep learning framework for cybersecurity enhancement in ERP systems integrated with big data*. *Journal of Cybersecurity and Information Protection*, 15(2), 112-129. https://doi.org/10.1016/j.jcip.06.011

[9] Vankayalapati, R. K., & Syed, S. (2020). Green Cloud Computing: Strategies for Building Sustainable Data Center Ecosystems. Online Journal of Engineering Sciences, 1(1), 1229. Retrieved from https://www.scipublications.com/journal/index.php/ojes/article/view/1229

[10] Manikanth Sarisa, Venkata Nagesh Boddapati, Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Shravan Kumar Rajaram.Navigating the Complexities of Cyber Threats, Sentiment, and Health with AI/ML. (2020). JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 8(2), 22-40. https://doi.org/10.70589/JRTCSE.2020.2.3

[11] Nguyen, M., & Patel, *Integrating deep learning models to optimize cybersecurity protocols in big data-enabled ERP solutions*. *IEEE Transactions on Cybersecurity*, 14(1), 45-59. https://doi.org/10.1109/TCS..0125

[12] Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020). Unveiling the Hidden Patterns: AI-Driven Innovations in Image Processing and Acoustic Signal Detection. (2020). JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 8(1), 25-45. https://doi.org/10.70589/JRTCSE.2020.1.3.

[13] Hemanth Kumar Gollangi, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Janardhana Rao Sunkara and Mohit Surender Reddy. (2020). "Echoes in Pixels: The intersection of Image Processing and Sound detection through the lens of AI and Ml", International Journal of Development Research. 10, (08),39735-39743. https://doi.org/10.37118/ijdr.28839.28.2020.

[14] Vaka, D. K. (2020). Navigating Uncertainty: The Power of 'Just in Time SAP for Supply Chain Dynamics. Journal of Technological Innovations, 1(2).

[15] Mandala, V. (2019). Optimizing Fleet Performance: A Deep Learning Approach on AWS IoT and Kafka Streams for Predictive Maintenance of Heavy - Duty Engines. International Journal of Science and Research (IJSR), 8(10), 1860–1864. https://doi.org/10.21275/es24516094655