Kurdish Studies
December 2022
Volume: 10, No: 2, pp 665-674
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

DOI: 10.53555/ks.v10i2.3668

Exploring the Role of Neural Networks in Big Data-Driven ERP Systems for Proactive Cybersecurity Management

Purna Chandra Rao Chinta[1*], Niharika Katnapally[2], Krishna Madhav Jha[3], Varun Bodepudi[4], Suneel BabuBoppana[5], Manikanth Sakuru[6]

[1*]Microsoft, Support Escalation Engineer
[2]Amazon, BI Developer
[3]Topbuild Corp, Sr Business Analyst
[4]Applab Systems Inc, Computer Programmer
[5]iSite Technologies, Project Manager
[6]JP Morgan Chase, Lead Software Engineer

Abstract
The use of artificial intelligence and machine learning, particularly neural networks, has effectively directed an increase in data-driven solutions and applications in different domains. Unfortunately, enterprise resource planning (ERP) vendors' emphasis on the importance of data integrity means ERP systems are less likely to protect themselves proactively through data analysis or by deploying external software with access to the data they maintain or process. Wholesale export of employee and business data into a data platform makes it possible for the ERP system and other business systems to use encryption and AI/ML software to proactively manage cybersecurity. This paper develops a conceptual framework for big data-driven ERP security management and uses it in six case studies. We found that applying a good enough simple learning model with the simplest network architecture will succeed in unmasking patterns that are more likely to have been overlooked. The case studies suggest that implementing big data-driven ERP cybersecurity will not significantly add software or maintenance costs, but harnessing artificial intelligence and machine learning services such as neural networks will add significant value to ERP customers.

Keywords: Artificial intelligence, big data, enterprise resource planning, machine learning, neural networks, security management , big data, cybersecurity, ERP, neural networks.

1. Introduction

Enterprise Resource Planning (ERP) systems have become the first place where user interaction with informational application programs occurs. These programs hold a conglomerate of all company information that affects the reliability of the entire computer network. That is why the fight against ERP cybercrime has become important to users. In big data-fueled ERP systems, proactive cybersecurity management is assisting with dealing with potential threats. However, fake cybersecurity facts increase the difficulty of enterprise security decisions. Now cybersecurity deals with the handling of a large number of threats, and these are also unknown threats; something that often translates into bad news for big data-driven ERP systems. The integration of machine learning technologies into ERP systems can better detect, recognize patterns, and classify potential cybersecurity concerns. This paper appraises the changes that the neural network framework introduces into the 'big data' realm and examines the potential benefits and considerations of machine learning technologies when enabling proactive cybersecurity management. It is also a warning of the reason why the happiness that artificial intelligence used in enterprise cybersecurity may have some unexpected consequences.The integration of machine learning technologies into Enterprise Resource Planning (ERP) systems holds significant promise for enhancing cybersecurity management in the age of big data. Machine learning, particularly neural networks, offers the ability to detect anomalies, recognize patterns, and classify potential cybersecurity threats with greater accuracy and speed than traditional methods. These technologies can proactively identify vulnerabilities and respond to unknown threats, making them vital for safeguarding the vast amounts of sensitive data stored in ERP systems. However, the growing reliance on machine learning for cybersecurity also presents challenges. Fake cybersecurity facts and misinformation can complicate decision-making processes, leading to misjudgments or overconfidence in automated systems. Furthermore, while AI and machine learning technologies offer impressive capabilities, they may also introduce unexpected consequences, such as new vulnerabilities or unforeseen errors. As such, organizations must approach the integration of AI in ERP cybersecurity with caution, balancing its potential benefits with careful oversight to avoid compromising system integrity.

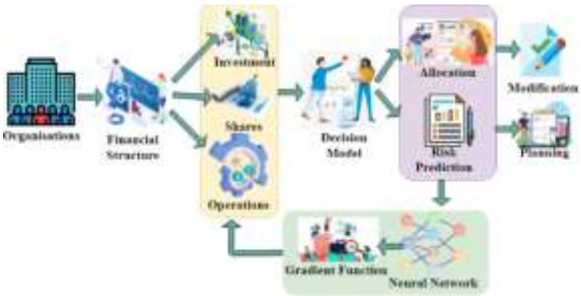


Fig 1: Optimized backpropagation neural network for risk prediction in corporate financial management

1.1. Background and Rationale

Enterprise Resource Planning (ERP) systems are essential for businesses today, as they provide a variety of business processes with a unified approach. An ERP system can collect data on production, account management, financial and human resources, and process and save it on server-based data hosting platforms. Due to this broad integration, businesses can benefit from an array of functionalities such as better daily operations, audit management, complex analyses, and more. ERPs usually manage large volumes of beneficial data, which in contemporary times has become a significant target for cybercriminals. Company and personal data can be accessed using the right skills and tools, posing a critical cybersecurity challenge for businesses. To preserve their integrity and signals, information needs to be securely sealed and customizations constantly protected. Hence, the quest for big data-driven proactive cybersecurity solutions has attracted attention over the past decade.

Proactive security involves capturing the best line of action quickly to address potential security threats. This implies that instead of "cleaning up" an already attacked system and stabilizing it to guarantee the availability and integrity of a security compliance model, a new strategy is proposed. Several ERP standard tools may be sufficient in avoiding any assault. For successful proactive cybersecurity planning, a large volume and diversity of data may be required. To this aim, advanced big data technologies have been explored. Of these cutting-edge methods, artificial neural networks stand out as they have demonstrated outstanding comprehension abilities. By uncovering complex correlations between various types of security data, these networks will counteract potential threats facing a business, such as viruses and denial of service schemes.

1.2. Research Objective

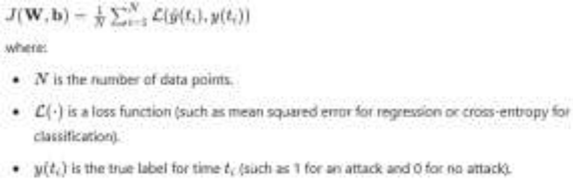
The research objectives to explore the role of neural networks in big data-driven ERP systems for proactive cybersecurity management are: - To critically examine system theory and cybernetics to comprehend the multifaceted and dynamic nature of cyber threats resulting from emerging business technology trends, increasing information sharing, accelerated globalization, vanishing perimeters, outdated regulations, layers of web vulnerabilities, and high-speed performance requirements. - To review literature on data warehousing, big data management, and ERP systems, along with fast artificial neural networks, particularly focusing on their ability to deliver real-time predictions during big data analysis. - To analyze high-level solutions to heterogeneous data integration and preprocessing, big data types, exploration, analytics and visualization techniques, prediction machines, evaluated attribute values, neural network training, and model validation, along with security policy development for staff and access management, incident and disaster recovery, and external activity monitoring in comprehensive ERP system architecture. - To extend a feasibility study on integrated big data-driven neural network facilities, together with their security feedback loop, for ERP systems that prove that security controls and compliance can be effectively and proportionately matched to managed security threats. - To analyze the qualitative differences in the features and outcomes of newly extending big data-driven neural network facilities for ERP systems that have recently provided significant business benefits in big data management, processing, exploitation, and visualization in typically concise and insightful chapters on these extremely large and complex subjects.

1.3. Scope and Significance

ERP security is a very complex issue and involves many tasks, processes, methods, technologies, tools, concepts, architectures, systems, measurements, standards, models, deployment groups, assessments, compliance processes, audits, definitions, and policies. This paper provides comprehensive coverage of the function of NEURONS and how it can be used in big data-driven ERP systems for proactive cybersecurity by ERP vendors, their implementation partners, developers, integrators, consultants, and end-users. Almost all researchers and practitioners have emphasized how cognitive computing can be adopted to help detect and remediate ERP security issues. However, they have not provided any substantive picture using a mature emerging function like NRFNNS and the associated proactive unified big data-driven ERP systems that are currently in use.

The role of NRFNNS is applicable to very large systems in any field. It is known to result in higher accuracy rates and reliable output. There are many use cases of NRFNNS with which the reader may be unfamiliar. We describe an interdisciplinary approach in a very complex context in the fields of cyber systems, artificial intelligence, predictive modeling, machine learning models, random forest architecture models, deep learning models, artificial neural network models, and business functions using the general systems theory approach. AI fields such as machine learning models, big data-driven systems, advanced cybersecurity using NRFNNS architecture, fortification of embedded systems, and other ERP security settings are also discussed to enhance the learning process. Learn how data for NRFNNS can be managed. Use the implementation of big data-driven systems to handle the cybersecurity ERP settings in very large enterprise environments. Knowledge of the roles of many components is part of the big data-driven systems for an ERP sophisticated cybersecurity management setup into which NRFNNS has been embedded. Understand the larger picture for high levels of ERP security to test the true limits of big data technologies using artificial intelligence. Results show that it has big data-driven generalization capability.

Equ 1: Cost Function for Training



$$J(\mathbf{W}, \mathbf{b}) = \frac{1}{N} \sum_{i=1}^{N} \mathcal{L}(\hat{y}(t_i), y(t_i))$$

where:

- N is the number of data points.
- $\mathcal{L}(\cdot)$ is a loss function (such as mean squared error for regression or cross-entropy for classification).
- $y(t_i)$ is the true label for time t_i (such as 1 for an attack and 0 for no attack).

2. Big Data-Driven ERP Systems

Today, the large scale of successful companies is mostly powered by big data in Enterprise Resource Planning (ERP) systems. It stands to reason that ERP systems are bound to include the past, present, and trends in the business data embedded in the data warehouse, such as 25 years of business experience in the industry, 20 years of sales data, 25 years of expenses data, 25 years of supply chain data, 20 years of human resource data, 20 years of IT budget, and many years of budget, and so on. Using big data and cyber resilience, ERP systems:

(1) Implement the predictive ERP special function.

(2) Build a utility function using big data analysis logic in the data warehouse, cloud DB, and large memory engine to support not only the current time but also a long time ago, e.g., more than twenty years.

(3) It can also be used for notification, transaction processing, instant messaging, decision-making agenda automation, self-tuning, and self-update in the special database and the concurrent index, thereby innovating the database and the concurrent index. For ERP users, it is protection of operations supported by the database and is burden-free, thereby gaining profits.In today's competitive business landscape, ERP systems leverage the power of big data and cyber resilience to provide unparalleled insights and efficiency. By integrating historical, present, and predictive data, these systems enable organizations to make informed decisions based on decades of industry experience and operational data. With advanced capabilities like predictive ERP functions, these systems can forecast future trends by analyzing over 20 years of data, including sales, expenses, supply chains, human resources, IT budgets, and more. Additionally, the integration of big data analysis, cloud databases, and large memory engines allows for seamless support not only of real-time operations but also long-term historical analysis. This innovative approach includes features such as automated decision-making, self-tuning, and self-updating databases, while ensuring concurrent index optimization. Through these advancements, ERP systems reduce operational burdens, enhance transaction processing, provide timely notifications, and safeguard businesses against disruptions, ultimately delivering greater profitability and business agility.

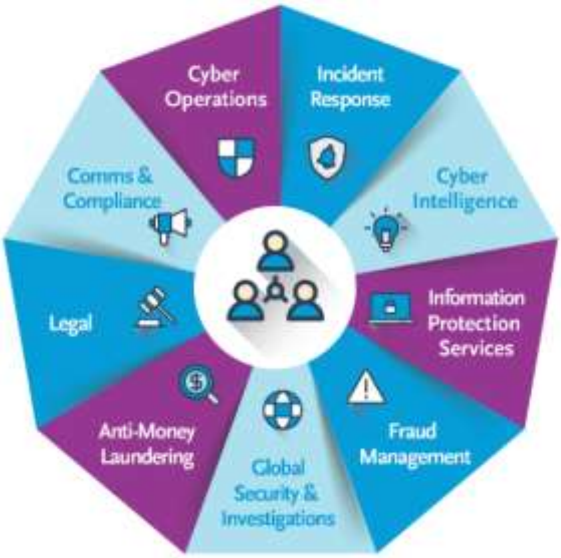


Fig 2: Data-driven cybersecurity

2.1. Overview and Components

As such, it is imperative to ensure the comprehensive protection of both the data and the operations performed by modern ERP platforms, which thereby require implementations of more advanced cybersecurity defense models in the form of threat detection, identification, and remediation systems. It is also this realization that has led to the construction of more proactive or predictive threat models that are able to anticipate as well as prevent such threats from compromising the confidentiality, integrity, and availability of ERP data and applications. This section provides a broad introductory overview of the neural network architectures that are leveraged towards the construction of predictive threat management systems in the domain of cybersecurity. At the same time, we shall also specify the unique components that form an NN architecture as well as offer a brief discussion of the operational principles that underlie the various components, especially the more recent developments in deep learning architectures that would further enhance NN-based threat management systems.

2.2. Challenges and Opportunities

For network-based ERP systems that analyze both sensor and business data, sophisticated fusion methods will be needed. Since there are so many variables and so much data to consider, the system will need to focus on specific operations for modeling and analysis. New types of time-series methods and alerting tools will be needed, since the many variables often change at different times and in different ways. ERP analytics solutions must support slowly developing but very complex data models, and the immense amount of real-time data gathering, filtering, and processing will challenge the performance of these tools. The 'big' nature of the business data to be analyzed will exacerbate frequently encountered IT system problems, leading to solution slowdowns and long processing delays before results are generated.

Big news will also bring some signs of good news. When periodic maintenance is being scheduled for a machine, or when some extreme production quality occurs, often associated with the end of a power-down period, there should be many real-time evidence pieces somewhere in the vast amount of sensor data available. Different-looking attacks, such as those on the ERP enterprise model or on the execution of some non-actual legal requirement operation, might also be observed, especially if hard-to-execute authorization expansion, brute force password guessing, attack mutiny, and unauthorized user escalation are entertained. Certain classes of threats could be eliminated without any analysis.

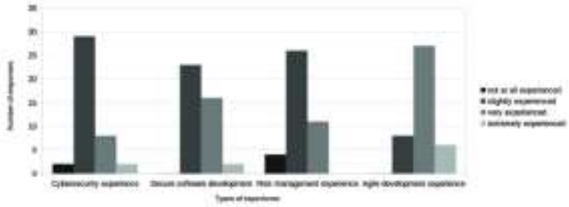


Fig : Clustered bar chart to show the cybersecurity self-assessment overview

3. Neural Networks in Cybersecurity

For organizations considering deep learning as a cybersecurity tool, the implementation of neural networks at the model level may be of interest. This is especially true considering that data available to companies for cybersecurity purposes has grown dramatically in recent years, and this data is characterized by variables that are constantly growing in number and complexity. Employing neural networks in enterprise systems helps in developing systems that are responsive to these characteristics. One common neural network model used in cyber forecasting is the shallow feedforward backpropagation neural network, which has performed well in detecting malware. In a typical neural network model, the inputs, hidden neurons, and outputs have a specific functional correlation mainly given by weights, biases, and thresholds.

This predictive model performs well in the context of deep learning because it leads to the generation of substantial amounts of generated data. As a result, for a significant bandwidth and a large volume of data, ERP systems, which are oriented towards Big Data and at least Level 3 artificial intelligence, can deploy this model even in root predictive conditions. Introducing neural networks at high levels of artificial intelligence may also allow for the design and development of security management models that, in general, are characterized by recursive security controls of large volumes of current data relevant to organizational life. Several machine learning and intelligent data analysis predictive models are based on neural networks.

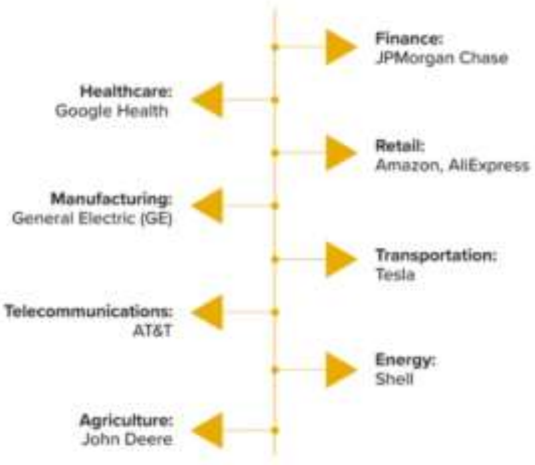


Fig 3: Artificial Neural Networks

3.1. Fundamentals of Neural Networks

Artificial neural networks (ANNs) were first proposed in 1943. ANNs are widely used in predictive analysis, data classification, character recognition, signal processing, and control applications. ANNs are also capable of recognizing patterns and interpreting complex relationships. Since ANNs do not require knowledge of mathematical descriptive models of the analyzed data, they are often called data-driven methods. The fundamental structure of a neural network consists of three types of neurons or nodes: input nodes, hidden nodes, and output nodes. The input layer is initialized with the input data, which are then transformed and output as desired based on the algorithm type. The data in the input layer, in the form of an N-dimensional input vector, is selected. This vector is defined by Variable(x1, x2, ..., xn), also called the independent variable. The distance between the second and last hidden layers can be free or multi-layer and is used to fix the complexity of the network. The more hidden layers there are, the higher the complexity, the greater the computational cost, and the higher the probability of overfitting.

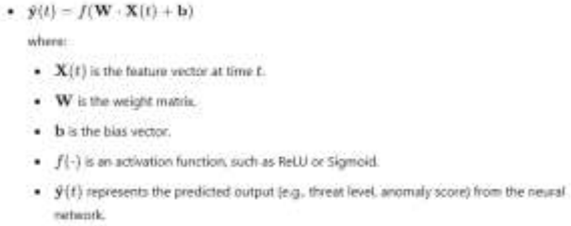
The output layer, after transforming the input vector and running weight optimization as described by the learning algorithm, will yield the result in the form of an S-dimensional output vector. This vector can have single or multiple dimensions as per the requirements of the algorithm. The output vector is a dependent variable or the result. Multiple (m > 2) output vectors mean multi-class classification, and m = 2 for a binary output vector called binary classification. Most neural networks can be summarized into considering different classes of modes. The output result is represented in the form of an ensemble probability plot for multi-class variables, a probability plot for binary classification, and a continuous-valued test response as the outcome for regression. Among these different classes, the overfitting and local minimum issues are resolved by tolerance, normalized, and auto-scaled data.

3.2. Applications in Cybersecurity

As the digital divide between corporate networks and cyberspace entities such as the web gradually lessens, the onslaught of traditional as well as sophisticated novel threat entities continues. Attempts to manage resultant risks through preventative, reactive, and offensive strategies have led to significant growth in terms of governance, legal compliance, technology controls, and security products aligned with cryptanalytics, firewalls, and antivirus capabilities. Systematic implementation of knowledge management approaches alongside big data technologies in the context of advanced cybersecurity platforms can do even better. Artificial intelligence methods such as neural networks that are modeled upon the human nervous system might serve as viable tools for inspection, analysis, and protection of sensitive information assets. Knowledge discovery in databases suggests that certain patterns, relations, or dependencies for information storage, creation, or usage can be identified using artificial intelligence.

Data mining techniques on a large scale, such as neural networks, can potentially serve the enterprise in the process of vulnerability assessment, trend predictions, risk management, and security activities enforcement. The technology of neural networks has already been abused, where the technology has become a threat in itself due to the onset of adversarial attacks. Such models are known to produce poor decisions due to various forms of errors including those derived from random noise or label contamination. Incrementally upgraded systems that can accommodate the capabilities of reason, logic, and perception in the field of cybersecurity warfare can potentially serve as proactive cyber defense mechanisms for organizations, societies, and national economies.

Equ 2: Neural Network Model for Anomaly Detection



- $\hat{y}(t) = f(\mathbf{W} \cdot \mathbf{X}(t) + \mathbf{b})$

  where:

  - $\mathbf{X}(t)$ is the feature vector at time t.
  - $\mathbf{W}$ is the weight matrix.
  - $\mathbf{b}$ is the bias vector.
  - $f(\cdot)$ is an activation function, such as ReLU or Sigmoid.
  - $\hat{y}(t)$ represents the predicted output (e.g., threat level, anomaly score) from the neural network.

4. Integration of Neural Networks in ERP Systems

In this section, the focus is laid on the integration of artificial neural networks (ANNs) in enterprise resource planning (ERP) systems. The design of ANNs is used to improve decision-making processes, as well as to optimize resource consumption in the automation of business activities. ANNs belong to the class of data-driven algorithms and have the capability of performing complex dynamic modeling with ease. Among business intelligence tools deployed in modern organizations, data mining fits into ANNs, which are very powerful predictive and analytical tools. ANNs have been considered in the analysis of ERP systems in different ways.

This is achieved through the performance optimization of commercial tool interfaces provided with ERP module support and the utilization of data and content provided by these systems. Early accounting applications designed to facilitate decision-making were established from knowledge derived from historical records. However, this demands wait times for production timing, as simplified or enriched knowledge is derived from computerized accounting systems. Research and development move towards more sophisticated models where actual system processes are used to predict or prescribe the decisions themselves. This leads to the creation of data warehousing systems that provide multidimensional analyses to develop meaningful knowledge with rich decision support capabilities. Neural networks contribute by providing a learning capacity, an aspect that other data mining techniques do not offer. The popularity of these technologies is making them more pervasive in support roles, particularly in enterprise resource planning (ERP).

4.1. Benefits and Challenges

Big Data in Enterprise Resource Planning (ERP) systems is continuously growing, which greatly influences the proactiveness and efficiency of real-time cybersecurity management in different organizations. To evolve and minimize the impact of advanced threats to the ERP system, businesses need to retune and redesign existing resources to keep pace with modern technology advancements. Neural network techniques and Big Data analytics in ERP support prospective insights for cybersecurity domain innovation for different organization services. The proposed model needs to capture and prioritize the most critical feature sets in an ERP system to maintain its integrity, security, and confidentiality, serving as a portfolio for real-time monitoring of log management and information classification, which facilitates automated risk analysis in achieving significant and improved protection.

Big Data-driven ERP systems enhance the overall organizational facilities and provide access internally and externally. However, real-time information security is the domain where security risks come to the fore as more users and businesses emerge. Maintenance and management of confidentiality, integrity, and availability of the data are the primary information security concerns for Big Data-driven ERP systems. As Big Data in ERP becomes a significant factor in supporting organizational management decisions, it also leads to different sorts of vulnerabilities and security threats. To enhance system security, disruption risk management, operational effectiveness, and ERP system real-time log management are necessary to propose automated security information and event management functionalities. In this regard, implementing an anomaly-based cybersecurity approach is an imperative action to identify and diagnose sophisticated attacks on data information systems. However, there are still various obstacles that hinder this important implementation.

Higher Productivity and Efficiency
Evolving Decision-Making
Better User Experience
Supply Chain Revolution
Better Customer Support

Fig 4: Benefits of AI in ERP Systems

4.2. Case Studies

This section introduces a case study-based demonstration of the logic and advantages of incorporating CNN and RNN into big data-driven ERP systems for proactive cybersecurity management. In this study, four real-world cybersecurity case studies pertaining to anomaly detection, policy enforcement, knowledge customization, and behavioral biometrics are conducted. Furthermore, the demonstration is implemented based on the public and private cloud infrastructures. As for the public cloud, a commercial-grade, high-reliability, and secure operating environment for implementing the ERP systems is utilized. For the private cloud, a deployment serves as the private and independent environment for external access restriction. The configurations of the training deep learning models are VGG16 and TS-LSTM; the training data are predisposed, the training results confirm the efficacy of the proposed neural networks, and the risk factor Z is defined as Z = P(model detecting system attacks and misusing confidential information and the privacy model being seriously defective) so that users can receive recommendations only when a Z value exists.

Sensing the spirit of teamwork, the absence of oversight in the password policy enforcement of Company X is reported. Employees may share passwords, enter the system with unauthorized identities, log in to the system with internal and external roles in parallel, and conduct personal activities at work. With this superior position, one person can be in between and pretend to be two people, so others believe in their every word. With the advanced capabilities inherent in ERP systems, organizational users and departments can be notified with the support of big data and achieve flexible and powerful policy deployment that automatically takes the company's rules into account.

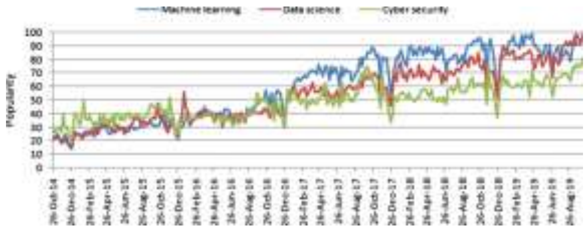


Fig : Cybersecurity data science: an overview from machine learning perspective

5. Proactive Cybersecurity Management

Growing concerns about cybersecurity are caused by the increasing number of discovered vulnerabilities that lead to unauthorized access, eavesdropping, spying, tampering, and the loss of information. These problems exist not only for sensitive military and civilian agencies but also for business organizations. Security experts have been responding to a sharply growing number of assaults against American governmental and business organizations. Business travelers using commercial laptops and wireless LANs are at risk for data theft and malicious insertion of information on these nodes. Cyber safety must be rigorously viewed not only in terms of intruders but also in terms of employees, no matter how well trained they are. In particular, companies' financial information, human resources, and customer databases should be viewed as primary targets for unauthorized access and tampering.

In the traditional method of incident handling, examining large amounts of system data is often a manual and time-consuming process and is often carried out after an adverse incident has already occurred. In general, organizations lack adequate techniques for either rapidly detecting security problems within the IP systems or reacting to security-related incidents whether intentional or accidental. These problems occur because an increasing amount of security-related data requires examination. Recognition of a large failure gap has led to the appearance of new network security products. These products can provide improved capacity to analyze large amounts of system logs, to correlate network security events, to visualize anomalies, and to react to security incidents.

EARLY IDENTIFICATION OF RISKS
ENHANCED REPUTATION AND TRUST
SUSTAINABLE GROWTH
COST SAVINGS
IMPROVED DECISION MAKING

Fig 5: Proactive Risk Management

5.1. Concepts and Strategies

Big data analytics is rapidly changing the landscape of business intelligence and enterprise resource planning systems. The grand vision of big data-driven ERP systems is to exploit the value derived from big data, fueling the enhancement of decision-making quality for business tasks not only in ERP operations but also in enterprise management. We attempt to pave the way toward enlightening the field of integrating advanced big data analytics capabilities into ERP systems, primarily from the perspective of proactive cybersecurity management, while specifically featuring and discussing the roles of neural networks. By merging multi-domain transdisciplinary knowledge in the fields of cybersecurity, big data analytics, advanced neural network techniques, and ERP with concerns on primary business operating tasks and enterprise system integrations, we aim to gain data-driven insights and subsequently transform them into intelligent technologies.

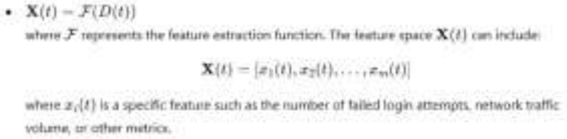
In line with the theme of this issue, we propose to draw attention to how to embed neural networks deployed with big data analytics capabilities into ERP systems for proactively managing cybersecurity operation tasks. Despite the appealing transparency of either some simple neural network models or some innovative strategies in making hard-to-understand models interpretable, the empirical understanding of how neural networks actually function behind the scenes, especially in some innovative designs of combining them with big data processing and entity implicational causality within different business operating contexts, is still limited. The fulfillment of this mission essentially requires further improvements not only in technical innovation but also in ensuring multi-stakeholder participatory cooperation and commitments to responsible actions.

5.2. Importance in Modern Organizations

Modern organizations use ERPs mainly for cost optimization and increased efficiency. Furthermore, ERPs can be used as tools for strategic decision-making. Modern ERPs are equipped with advanced business intelligence tools that allow them to provide information in the form of descriptive as well as predictive analytics. These advanced features, along with the modern Big Data-driven ERPs, help organizations in the area of proactive cybersecurity and make them more resilient to the ever-increasing security threats. Neural networks, which are capable of self-learning and providing predictions, play a vital role in the business intelligence modules of modern, Big Data-driven ERPs. These neural networks can be used to a great extent in the areas of predictive and prescriptive analytics to provide cybersecurity insights on a proactive and real-time basis. As a result, this allows organizations to make strategic decisions that make them resilient to cybersecurity threats.

In the case of organizations that use separately architected Big Data platforms, they pose challenges with regard to data sharing between the main ERP and the Big Data platforms. However, advancements in technology are aimed at integrating Big Data and ERP technologies because ERPs that are integrated with Big Data can function as hyper connectors to strategic decisions, leveraging analytics and technologies like machine learning, AI, business intelligence, and neural networks. At the same time, advancements in Big Data and ERP technologies, along with cloud computing or on-premises architecture, will help the security team adopt a new focus built around self-learning, AI, and security insights that are capable of detecting advanced threats in real-time.

Equ 3: Feature Extraction and Preprocessing



- $\mathbf{X}(t) = \mathcal{F}(D(t))$

where $\mathcal{F}$ represents the feature extraction function. The feature space $\mathbf{X}(t)$ can include:

$$\mathbf{X}(t) = [x_1(t), x_2(t), \ldots, x_m(t)]$$

where $x_i(t)$ is a specific feature such as the number of failed login attempts, network traffic volume, or other metrics.

6. Conclusion

Current enterprise resource planning systems facilitate a comprehensive overview of business activities and enable data sources integration for an automatic data update without redundant tasks or data errors. With the advent of big data, companies are now able to match and integrate data via different information systems. However, the various facts of dispersed data, diverse data architectures, and distinct data descriptors resulted in difficulty in terms of data integration. Consequently, this research extends ERPs with a big data architectural concept and utilizes neural networks to automatically align the urban aspects addressed by plant-specific or company-specific security ecosystems. Our study introduces the security-related paradigms that would likely play a key role in the ongoing enhancement performance and functioning of the ERP big data. Moreover, the architectural diagram that has been proposed aids the security. It suggests better insights concerning ERP usability contributors that can support ongoing updates aimed at cleaning the ERP for big data advantage. By ensuring the goals of industry 4.0 and a society of smart data for avoiding unlikable potential data misuse, the framework represents an interpreted cultural cybersecurity-related tool addressing a better work-life balance. The system incorporates aspects such as mutual confidentiality, accurate monitoring, data correctness, and insults through diverse non-bank activities and input restriction to stop data hacking. The mentioned concept supports better monetary planning, inventory forecasting, supply chain management, price and revenue forecasting, asset security, production management, and customer relations. Our focal application covers the interrelationships among big data and big data analytics in the first place related to ERP evolution. Subsequently, we analyze direct cybersecurity and its prospects.

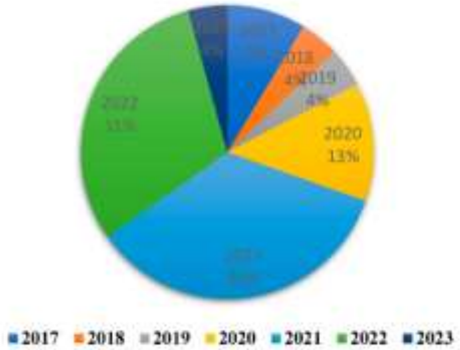


Fig : Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection

6.1. Summary of Findings

The fundamental aim of this study was to explore the role of neural networks in relation to big data processing and management within an ERP system in the form of proactive cybersecurity management. It was firstly noted that while business intelligence technology may produce large volumes of data that are capable of being processed at high speeds, it remains difficult to make predictions or to suggest improvements when utilizing only a small fraction of the data. This can be a hindrance in relation to proactive or predictive management, which is a desirable feature of any business process, including cybersecurity management.

The use of neural networks in business intelligence-compartmentalized ERP systems can reduce exposure times to potential cyberattacks, protect information, detect intrusion attempts and, in doing so, enhance decision-making processes and lead to insight generation. Reduced exposure times are achieved by detecting quicker, more complex, and hidden patterns through the pre-analysis of critical data and by generating an alert in real time. The defense of crucial information is also obtained through the secure pre-analysis of critical data. Lastly, the detection of a broadening of possible intrusion attempts is established through the identification of specific attack patterns based on particular requirements. The incorporation of neural networks within an ERP system also has beneficial implications with the expansion of business intelligence.

6.2. Future Trends

In this section, the future of cybersecurity using Big Data and neural network techniques is discussed, which will be needed in ERP systems for maintaining their performance and efficiency. As existing ERP system users, such as corporations, witness the rapid development and technological applications of Big Data technology, they expect its assistance in handling exponential data growth effectively. It is believed that cybersecurity will receive more attention, which may be regarded as a low-risk investment given the current high Internet usage of normal ERP systems. Additionally, with the rapidly increasing number of IoT devices and services, the cybersecurity of ERP systems should be considered a top priority, where neural networks will become an essential part of Big Data modeling frameworks for identifying security vulnerabilities and detecting potential cyber threats. Information sharing and accountability are also worth exploring in future studies concerning the security of Big Data-empowered cyber-physical ERP systems comprising the integration of other enabling technologies. Meanwhile, a systematic analysis of the intelligent cybersecurity model involving all of the integrated technologies in the cyber-physical system is missing. It is promising that smart cyber-physical ERP systems will become a possibility for enterprises with the rapid introduction of the aforementioned technologies. Gleaning from the cyber-physical system security field, the adoption of isolated protections is strongly discouraged. Among the various concerns that need to be addressed in the realm of secure design, ensuring adequate data distribution and analysis, serious considerations for using Big Data are necessary.

7. References

1. Syed, S. (2022). Breaking Barriers: Leveraging Natural Language Processing In Self-Service Bi For Non-Technical Users. Available at SSRN 5032632.
2. Nampally, R. C. R. (2022). Neural Networks for Enhancing Rail Safety and Security: Real-Time Monitoring and Incident Prediction. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 49–63). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2022.1155
3. 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
4. Rajesh Kumar Malviya , Shakir Syed , RamaChandra Rao Nampally , Valiki Dileep. (2022). Genetic Algorithm-Driven Optimization Of Neural Network Architectures For Task-Specific AI Applications. Migration Letters, 19(6), 1091–1102. Retrieved from https://migrationletters.com/index.php/ml/article/view/11417
5. Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. International Journal of Engineering and Computer Science, 11(08), 25618–25631. https://doi.org/10.18535/ijecs/v11i08.4698
6. Syed, S. (2022). Integrating Predictive Analytics Into Manufacturing Finance: A Case Study On Cost Control And Zero-Carbon Goals In Automotive Production. Migration Letters, 19(6), 1078-1090.
7. Nampally, R. C. R. (2022). Machine Learning Applications in Fleet Electrification: Optimizing Vehicle Maintenance and Energy Consumption. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.8258
8. Vaka, D. K. (2020). Navigating Uncertainty: The Power of 'Just in Time SAP for Supply Chain Dynamics. Journal of Technological Innovations, 1(2).
9. 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).
10. Kumar Rajaram, S.. AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance. In Educational Administration: Theory and Practice (pp. 285–296). Green Publication. https://doi.org/10.53555/kuey.v28i4.7529
11. Syed, S. (2022). Leveraging Predictive Analytics for Zero-Carbon Emission Vehicles: Manufacturing Practices and Challenges. Journal of Scientific and Engineering Research, 9(10), 97-110.
12. [12] RamaChandra Rao Nampally. (2022). Deep Learning-Based Predictive Models For Rail Signaling And Control Systems: Improving Operational Efficiency And Safety. Migration Letters, 19(6), 1065–1077. Retrieved from https://migrationletters.com/index.php/ml/article/view/11335
13. Vaka, D. K. " Integrated Excellence: PM-EWM Integration Solution for S/4HANA 2020/2021.
14. Sarisa, M., Boddapati, V. N., Kumar Patra, G., Kuraku, C., & Konkimalla, S. (2022). Deep Learning Approaches To Image Classification: Exploring The Future Of Visual Data Analysis. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.7863
15. Syed, S. (2022). Towards Autonomous Analytics: The Evolution of Self-Service BI Platforms with Machine Learning Integration. Journal of Artificial Intelligence and Big Data, 2(1), 84-96.
16. Nampally, R. C. R. (2021). Leveraging AI in Urban Traffic Management: Addressing Congestion and Traffic Flow with Intelligent Systems. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 86–99). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1151
17. Vaka, D. K. "Artificial intelligence enabled Demand Sensing: Enhancing Supply Chain Responsiveness.
18. Venkata Nagesh Boddapati, Manikanth Sarisa, Mohit Surender Reddy, Janardhana Rao Sunkara, Shravan Kumar Rajaram, Sanjay Ramdas Bauskar, Kiran Polimetla. Data migration in the cloud database: A review of vendor solutions and challenges . Int J Comput Artif Intell 2022;3(2):96-101. DOI: 10.33545/27076571.2022.v3.i2a.110
19. Syed, S. (2021). Financial Implications of Predictive Analytics in Vehicle Manufacturing: Insights for Budget Optimization and Resource Allocation. Journal Of Artificial Intelligence And Big Data, 1(1), 111-125.
20. [Aravind, R., Shah, C. V., &amp; Surabhi, M. D. (2022). Machine Learning Applications in Predictive Maintenancefor Vehicles: Case Studies. International Journal of Engineering and Computer Science, 11(11), 25628–25640.https://doi.org/10.18535/ijecs/v11i11.4707
21. Danda, R. R. (2021). Sustainability in Construction: Exploring the Development of Eco-Friendly Equipment. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 100–110). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1153
22. Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Kiran Polimetla. An analysis of chest x-ray image classification and identification during COVID-19 based on deep learning models. Int J Comput Artif Intell 2022;3(2):86-95. DOI: 10.33545/27076571.2022.v3.i2a.109
23. Mandala, V., & Mandala, M. S. (2022). ANATOMY OF BIG DATA LAKE HOUSES. NeuroQuantology, 20(9), 6413.
24. Nimavat, N., Hasan, M. M., Charmode, S., Mandala, G., Parmar, G. R., Bhangu, R., ... & Sachdeva, V. (2022). COVID-19 pandemic effects on the distribution of healthcare services in India: A systematic review. World Journal of Virology, 11(4), 186.Nimavat, N., Hasan, M. M., Charmode, S., Mandala, G., Parmar, G. R., Bhangu, R., ... & Sachdeva, V. (2022). COVID-19 pandemic effects on the distribution of healthcare services in India: A systematic review. World Journal of Virology, 11(4), 186.
25. Korada, L. (2022). Using Digital Twins of a Smart City for Disaster Management. Journal of Computational Analysis and Applications, 30(1).

26. 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
27. Maguluri, K. K., Yasmeen, Z., & Nampalli, R. C. R. (2022). Big Data Solutions For Mapping Genetic Markers Associated With Lifestyle Diseases. Migration Letters, 19(6), 1188-1204.
28. Sondinti, L. R. K., & Yasmeen, Z. (2022). Analyzing Behavioral Trends in Credit Card Fraud Patterns: Leveraging Federated Learning and Privacy-Preserving Artificial Intelligence Frameworks.
29. Vankayalapati, R. K., Edward, A., & Yasmeen, Z. (2021). Composable Infrastructure: Towards Dynamic Resource Allocation in Multi-Cloud Environments. Universal Journal of Computer Sciences and Communications, 1(1), 1222. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/1222
30. Kothapalli Sondinti, L. R., & Syed, S. (2021). The Impact of Instant Credit Card Issuance and Personalized Financial Solutions on Enhancing Customer Experience in the Digital Banking Era. Universal Journal of Finance and Economics, 1(1), 1223. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1223
31. Subhash Polineni, T. N., Pandugula, C., & Azith Teja Ganti, V. K. (2022). AI-Driven Automation in Monitoring Post-Operative Complications Across Health Systems. Global Journal of Medical Case Reports, 2(1), 1225. Retrieved from https://www.scipublications.com/journal/index.php/gjmcr/article/view/1225
32. Maguluri, K. K., Pandugula, C., Kalisetty, S., & Mallesham, G. (2022). Advancing Pain Medicine with AI and Neural Networks: Predictive Analytics and Personalized Treatment Plans for Chronic and Acute Pain Managements. Journal of Artificial Intelligence and Big Data, 2(1), 112–126. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1201
33. Tulasi Naga Subhash Polineni , Kiran Kumar Maguluri , Zakera Yasmeen , Andrew Edward. (2022). AI-Driven Insights Into End-Of-Life Decision-Making: Ethical, Legal, And Clinical Perspectives On Leveraging Machine Learning To Improve Patient Autonomy And Palliative Care Outcomes. Migration Letters, 19(6), 1159–1172. Retrieved from https://migrationletters.com/index.php/ml/article/view/11497
34. Ravi Kumar Vankayalapati , Chandrashekar Pandugula , Venkata Krishna Azith Teja Ganti , Ghatoth Mishra. (2022). AI-Powered Self-Healing Cloud Infrastructures: A Paradigm For Autonomous Fault Recovery. Migration Letters, 19(6), 1173–1187. Retrieved from https://migrationletters.com/index.php/ml/article/view/11498