Journal of Artificial Intelligence and Big Data Disciplines (JAIBDD)

International | Peer Reviewed | Open Access | Online

Designing Neural Network Frameworks for Big Data Analysis in ERP Systems to Counter Cyber Threats

Zakera Yasmeen

Data engineering lead,

Microsoft Corporation,
Charlotte NC.

Abstract *:* The article outlines the development of neural network frameworks to counter future cyberattacks in Enterprise Resource Planning (ERP) systems. A lack of security can lead to major risks. Hence, an ERP system is more prone to cyberattacks. Many researchers have suggested the integration of big data analytics to counter cyberattacks. We have designed a neural network framework for binary classification to predict the attack classes in real-time. We have compared various types of neural networks to check which neural network is more effective and has less error in predicting cyberattacks. The findings revealed that out of the proposed methodologies, the ensemble of the Recurrent Neural Network as an autoencoder is the most effective design.

We proposed three designs, and we have found that the ensemble of deep learning provides a 97.5% error rate. This design is most effective for big data architecture in the real-time pipeline of ERP. The trends of deep learning work on big data but face some practical issues in implementing the models. The study is beneficial for organizations using ERP, which is the largest ERP vendor and the most costly product widely used worldwide. Hence, it provides research in the field of cybersecurity and contributes to the latest technology approach redesign for practitioners. Deep learning methodologies face practical challenges in the real-time representation of any event. The relevance of the computing approach of the novel and deep learning model in practice is identified, and it is performed by the researchers.

Key words : ERP Systems, Cybersecurity, Neural Networks, Future Cyber Attacks, Big Data Analytics, Attack Prediction, Binary Classification, Real-Time Pipeline, Recurrent Neural Network, Autoencoder, Deep Learning Ensemble, Big Data Architecture, Error Rate, Real-Time Representation, Practical Challenges, Cybersecurity Research, ERP Vendors, Technology Redesign, Predictive Models, Computing Approaches.

1. Introduction

Neural networks are transforming different methodologies to solve business problems on a day-to-day basis. In that list, big data analysis is very important in enterprise resource planning (ERP) systems. The ultimate aim of this survey is to design a simple and suitable neural network framework for big data analysis in ERP systems to counter cyber threats practically. Cyber threats always expose different vulnerabilities of enterprise resource planning (ERP) systems at different levels by compromising the endpoints of organizational information technology infrastructure. Security and performance protection are two sides of the same coin and have to be enhanced in ERP systems. The following two questions drive the research in this survey: 1) How to store and manage neural network training and testing data in a big data environment? 2) How to propose a simple and suitable neural network data analysis framework to counter vulnerabilities in the management and organization of human resources in an ERP system? For that, the survey is split into four sections. The introduction motivates the proposed approach. The second section presents the theoretical aspects. Within it, big data analysis and neural network data analysis are discussed. Then, we move to the final sections. First, the proposed framework is discussed from an application perspective. Then, a case study is presented. The conclusion wraps up the survey, giving the results and future directions for this work. The present survey focuses on the practical and theoretical analysis as well as the design of the framework. Moreover, all aspects have been compared and contrasted with the methodologies used in the field. In particular, it scrutinizes different use-case practices in an enterprise resource planning (ERP) system. In an organization, twenty-five percent of all cyber attacks are directly hitting enterprise resource planning (ERP) systems, resulting in significant financial losses for businesses.

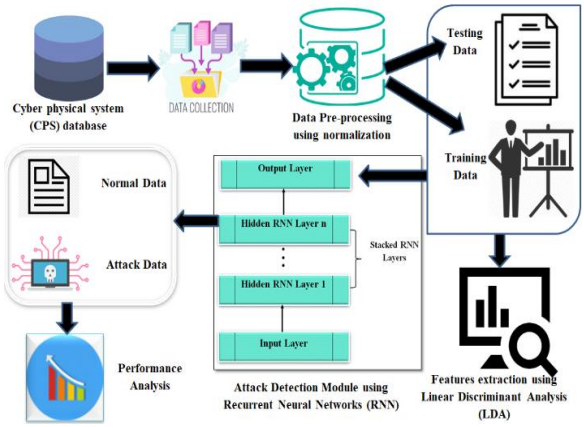

Fig 1 : Robust Deep Learning Based Framework for Detecting Cyber Attacks from Abnormal Network

1.1. Background and Significance

Enterprise Resource Planning (ERP) systems evolve with technological development and spread. As ERP tools have developed, so has the content of the functions, along with the speed of processing increasing cyber threats such as internal and external access attacks. In the evolving world of IoT technologies and 5G communication technologies, the extension of ERP to fields such as big data, machine learning, cryptographic technologies, and neural networks is inevitable. The term big data may refer to structured, semi-structured, or, as in today's conditions, unstructured data sets that are impossible to store and analyze using traditional database systems. There are two applications of big data for organizations. On the one hand, there is a dimension in which the storage and processing systems are difficult to handle by themselves. There is also a vast amount of information to be exploited by organizations.

In the big data process, providing infrastructure related to technologies such as data storage, organization, statistical and spatial analysis, and data mining management is defined as big data management. On the other hand, completely new opportunities can be explored by managing the information flow to be controlled timely and accurately. Cloud computing is important in big data in both the size of the analyses and the commercialization of the offer. As can be seen, big data opens a big new area and also includes difficulties and opportunities. To exploit these opportunities and turn them into strategies that will facilitate decision-making could be challenging, costly, and mostly to reap the potential of these investments. Therefore, advanced data techniques such as machine learning on enormous data have immense business opportunities, and it can be a severe drawback in terms of security issues. Designing neural network frameworks for big data is important in terms of countering it. Various applications of neural networks in ERP systems and data analytics can be found.

Equation 1 : Neural Network Model (Feedforward):

$$y = f(Wx + b)$$

y is the output,

x is the input vector,

W is the weight matrix,

b is the bias vector,

f is the activation function (e.g., ReLU, sigmoid).

1.2. Research Objectives

The main objective of the research study is to investigate how the design of neural network frameworks to support the use of big data analytics in contemporary enterprise resource planning systems can counter threats by learning from past activities. In line with the main objective of the research study, the following sub-objectives were formulated. Firstly, we outlined the need to study existing techniques and solutions to assess the influence of cybersecurity threats on big data analytics supported by neural networks in modern enterprise resource planning systems and to highlight benefits and challenges. Negligence towards active study in this focus area of cyber threats led the researchers to indicate the need to implement the principle of innovative data solution design. Secondly, among the external threats to data systems are mainly initiatives such as injection attacks, system data export, unauthorized changes, and encryption of system data. Among the most common is the unauthorized change which can be defined as imperceptible tunings of the flow of system events with simultaneous falsification of data already stored in data systems. The data integrity change is carried out in the direction of false-in-range events or incongruous events with historical data states. Examples of such activity are anomalies generated by innovations that are inseparable from the possibilities of big data analytics solutions. Anomalous activity is indicated as an unauthenticated factor that affects the analysis of stored data and the use of unusual patterns created by adversaries. According to the occurrence and causality of anomalies in the system data as proof of unauthorized activity in the system, data solutions are classified into the category of unsupervised data systems, where general business rules and acceptable data traffic patterns are learned. Models of the neural network system of this type are designed to perform the reconstruction or encoding of the features of the reconstructed database state. An example of such a model is the autoencoder.

The network adaptive abilities of the autoencoder allow it to refresh the stored state in enterprise resource planning database systems in real time without disconnecting the databases from users, demonstrating capabilities to offset the reversibility of cyber threats close to the user end. All empirical cyber solutions indicated have their technological limitations that reactionaries can render obsolete, thus the need to estimate their use in the big data analytics-neural network environments for enterprise resource planning systems in a state close to advanced prototype proof of operational usefulness. In the case of anomalies consisting of specific attacks such as unauthorized property transfers in enterprise resource

planning systems, temporal cyber analysis of unauthorized events and training of the autoencoder can be accelerated. It should be emphasized that no decision is yet final, and the angle of assessing threats with the prototype presented during the experiment further enables the highlighting of solutions to be corrected and enhanced. Taking into account the need to master a gradual research solution, the second research objective presented is the assessment of the possibilities and methods of training autoencoders in response to the coexistence of big data analytics in enterprise resource planning systems with fierce cyber warfare threats. Adjustments to the autoencoder will be developed and tested to measure its ability to provide real-time compensation for change, and some errors caused by the presence of data drift in enterprise resource planning systems are acceptable. Deep neural networks can also improve data visualization, exploratory analysis, and decision-relevant information. The envelope of the training set data for solving the classification of deep neural networks and autoencoders is also saved. Even though the autoencoder contains an error due to external persuasion, the enterprise resource planning systems are fundamentally unequal to training data or dependencies. This situation illustrates the interruption of the deep learning model construction cycle. Model validation will graphically expose the error and its accepted limit due to data drift in the system. Finally, future research will be planned based on the problem area found. At the same time, the way to resolve the defect will be modeled as a testing scenario.

1.3. Scope and Limitations

This paper is based on the premise that contemporary cyber threats do necessitate that all potential lines of thought in cybersecurity analyses be pursued, analyzed, and developed further to hopefully guard against these possibilities. It is important to keep in mind that some of the subject areas discussed also have profound theoretical implications. The primary scope of the paper, however, is to gather and summarize primary and secondary data to provide a method by which ongoing dedicated research in big data, neural networks, ERP systems, and the integration of each of these fields in counteracting cyber threats can be approached in a future comprehensive investigation. The primary focus of the paper is on the observation of big data analysis, neural networks, and ERP systems in the context of cyber threats, whereas any application, networking, and systems architecture considerations and approaches are beyond the scope of this paper. The research seeks to explore aspects of neural network system architectures, algorithms, and models, which might gain counterintuitive insights into the operation and challenges of state-of-the-art ERP systems when subjected to various forms of cyber attacks. However, care must be taken when a reader wishes to use the provided method to avoid leaping to conclusions that lead to systemic lock-in. Differential arms-race considerations are beyond the scope of this paper but have been borne in mind during the research process. This paper is limited primarily to the development and mitigation of data availability and access patterns. Data availability becomes a clear practical limitation that is beyond the ability to mitigate given that a 'real' operational cybersecurity setting might deal with strategic data and actors that are not conducive to statistical analyses due to the discrete complexity that does not lend itself to a regression-type analysis. The thorough cybersecurity requirements outlined in legislation in the countries of the researchers also precluded a level and trust for the analysis of data. Furthermore, operational cybersecurity complexity further includes end-to-end security, which makes data unfeasible.

2. Neural Network Frameworks in Big Data Analysis

Neural networks are computing systems inspired by the biological neural networks that constitute animal brains, which consist of as few as four nodes and as many as more than five million on modern systems. This is because their structure is an interconnected web of nodes, akin to a microcosm of computer operating systems. This structure allows the systems to adapt to changing input, generalize to unique datasets, and reveal intrinsic and hidden features of the data. Consequently, they are efficient for processing and analyzing large amounts of complex data or acting on certain unfavorable circumstances, a field known as big data. One of the main tenets of big data is its application to and implications for business and finance, from sentiment analysis to investment analysis, to threat detection and fraud protection.

One credit that can be given to neural networks' considerable success in the big data analytics area is, as mentioned, their adaptability. Another advantage of neural networks in such applications is their efficiency in capturing data as it becomes available. Ideally, neural network implementations are guided by and inform decisions about data, which can also manifest itself as decision-making based on data rather than other more classical and time-dependent decision-making in the absence of data. Knowing when to act if conditions indicate a threat based on continuously analyzed data is essentially a credit of neural networks and, more broadly, big data analytics. Neural networks operate in two forms, depending on what data is available—the more information there is, the more accurate the model; unsupervised and backed-up learning. A neural network that conducts supervised and unsupervised learning can infer, predict, and identify patterns as a result. Neural networks, in addition to their strength in anomaly detection, are often quite useful as predictive analytics tools. They can produce highly accurate and effective results, even better than other analytics systems, because of the large amounts of input. Hence, their use in identifying and predicting the occurrence of these threats, potentially before a hacker exploits a feature of the system, is a necessity.

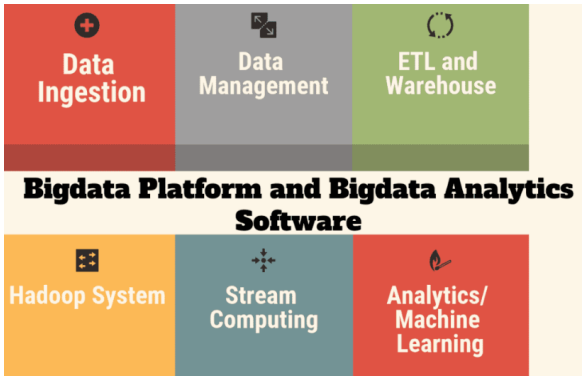

Fig 2 : Big Data Platforms and Big Data Analytics Software

2.1. Overview of Neural Networks

2.1 Overview of Neural Networks

Neural networks are a class of machine learning models designed after the structure and functions of human neurons. Artificial neural networks (ANNs) consist of several interconnected neurons or units arranged in layers. A unit has information that passes through it with several weights. These weights are adjusted during training, and algorithms in the neural networks are learned to adjust the weights. A multi-layered perceptron (MLP) constitutes one such class of neural network containing an input layer, some hidden layers, and an output layer. Each unit in a layer connects

to each unit in another layer and conveys output from one layer to another through the connection. However, the summation of inputs can saturate the network. Consequently, the research community incorporated a nonlinear function on the summation of inputs widely called activation. The activation function maps the weighted sum to the next unit in the network.

It is worth mentioning that each unit activation is represented as y_j = f(net_j), where y_j is the activation of the jth unit in the network, f is the activation function, and the net is the sum of the weighted data with their connections. Lately, several activation functions have been proposed to be the best, including the rectified linear unit, sigmoid, and tanh function. Training works through the sum of the inputs into the different layers of the neural network in the forward propagation net = ∑ x = 0 to n - 1 w - n x, where w are the weights of the neural network, x are the inputs to the neural network, and n is the number of inputs. After the inputs have been computed with weights for every neuron in the output layer, the signal works downwards through the network or the calculation of the backward propagation given by δ_j = [f(net_j) - t] of (j)', after this, the weights w are adjusted depending on the input x. The connectionists have shown these distinguishable neural network learning errors fully utilizing the backpropagation approach. With the capacity of the neural networks, the adaptation can be automatically consistent in detecting even the most subtle changes within the network systems during their operations, such as the ERP system as well as a sensor system. Despite its rapid dynamic developments, ANN also includes many distinct models that are receptive to specific data types, which also maintains its error rates. Therefore, in response to the strong demand for the existing ERP that continues improving its reliability and reduces internal cybersecurity threats, this research employs a backpropagation algorithm as a powerful learning algorithm to improve systems.

It was recognized that the backpropagation algorithm includes a system comprising neurons in various layers. The connections between the units or neurons possess certain weights that the learning algorithms unite in improving the net outputs to ensure maximal reliability of the system, including security against internal threats. There are four different layers. First, the input layer accepts the pattern or numerical values of a certain data set. Second, the hidden layer consists of influential nodes of a network that process information but have no direct participation in resolving the equation. Third, the output layer contains nodes that assist in detailing the analysis based on the input layers of the information. Additionally, they function in producing internal organizational threat reports. In summary, neural networks are capable of processing big data via the aforementioned characteristics; thus, processes in real time can produce correct decisions and forecasts.

2.2. Applications in Big Data Analysis

When discussing big data analysis in large organizations, neural network frameworks serve as a promising approach. Many applications of neural networks include, but are not limited to: predictive analytics, analysis of customer behaviors, analysis of time series data, predictive equipment maintenance, real-time data integration, pattern recognition, and anomaly detection. The use of such applications is not without success in discovering insights for organizational decision-making either. One similarity among many of the previous applications of neural networks indirectly mentioned above is their ability to effectively handle big data. Neural network frameworks can process data at a much quicker rate compared to traditional statistical analysis, even when it comes to extremely large datasets. They are appealing due to their nonparametric character and ability to understand and learn data patterns, behavior covariance, and the ability to automatically rank data patterns. For example, customer behavior clustering might result in numerous features. Industries such as retail and supply chain take advantage of implementing neural networks, particularly for voice recognition, customer intelligence, and digital supply chain real-time visibility systems. While many companies are currently exploring neural network frameworks, it is expected that this adoption will grow exponentially in the coming years as the prowess of artificial intelligence continues to be unleashed by academic researchers in numerous fields apart from information systems and SMEs in a variety of industries. Nonetheless, promising discoveries have already been made by scholars who discovered the boosting capability of MLPs for Enterprise Resource Planning data and that the improvements are attained by using a stochastic optimizer. Numerous other relevant areas and future research are outlined in this paper.

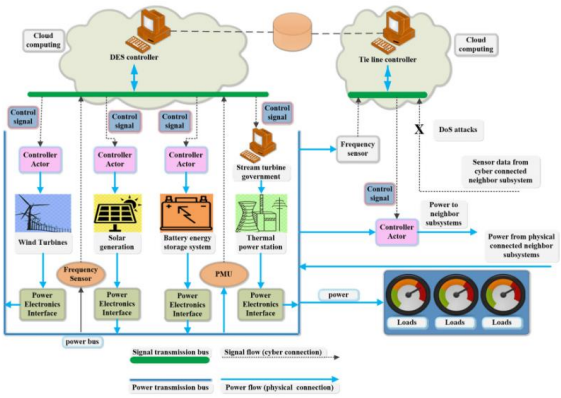

Fig 3 : Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems

3. Cyber Threats in ERP Systems

ERP is multitier, multifunctional software that integrates data, improves business processes, and manages resources. It is an integrated and automated system that facilitates the processing of real-time data. It enhances the flow of information within the organization. A cyber threat is an unintentional event that might cause harm to the system. Many threats have been identified, and their effects are studied. Some of the well-known threats are malware, trojans, phishing, insider threats, external hacking, denial-of-service attacks, and various e-attacks. Malware threats are of various types. The distributed denial-of-service attack is on the rise. Social engineering attacks and phishing attacks are on the rise. Phishing is a trick aimed at stealing users' sensitive information such as usernames, passwords, email addresses, and credit card numbers. Insider threats are more serious since a significant percentage of companies use ERP systems to support applications.

Data breaches are a major concern for data owners. A data breach can be devastating to organizations that rely on ERP systems. Data breaches cost organizations millions. Cyber infrastructure platforms have become vulnerable to attackers in cyberspace. The effect has alarmed organizations and prompted them to adopt robust security measures. Many real-world implications could result from the vulnerability of Enterprise Resource Planning systems in the industry. Ransomware encrypts data and asks for payment in exchange for the decryption key. Public-private key encryption is used in ransomware. Private key encryption is used to encrypt the victim's data. The victim's private key is sent to a command-and-control server for storage when the data has been encrypted. The attacker will provide the private key to the victim for a specific ransom amount to be paid. A large construction company faced a significant loss in its ERP framework due to data breaches and faced the disrepute of

investors and customers who had good terms with the company. Cybercriminals targeted vulnerable software in the past. A hacking group warned that if the ransoms were not paid in due time, customer data would be released. Various scams caused companies to contract with phased-based providers and later promised to sue the client after not giving the expected payout. A non-governmental organization was threatened by a group that claimed they had no intention to release the company's customer database; they still demanded a significant amount of money. Maintaining a secure framework in a digital environment requires more attention. Hence, reactive strategies are not sufficient to offer remarkable protection from existing and novel threats. Thus, a well-structured proactive distributed approach must be executed and sustained in conjunction with reactive strategies. Despite the extensive discussion on the pertinent topics, there is no evidence of empirical-based research in the field.

3.1. Types of Cyber Threats

Cybersecurity measures and planning are heavily informed by the nature of cyber threats. Unfortunately, hackers can probe the weak points of companies that use these systems by attacking enterprise resource planning (ERP) systems. Cyber-physical attacks of this scale threaten to subvert a significant portion of an organization's information systems. For organizations, this is a significant risk. Table 2 lists various types of cyber threats to an enterprise's ERP system, specifying the threats based on the actors implicated, i.e., whether the attackers are internal or external to the enterprise, and the motive for perpetrating the attack. The impact of the threats is high, involving whole business functions.

To genuinely understand cyber threats within ERP systems, we must classify cyber threats based on who is perpetrating the attack and the likely detrimental effects. The attacker can be either an insider or an outsider. An employed workforce misuse falls into the insider category, whereas an external attack is typically carried out by someone who has no direct connection to the organization, either singularly or with the help of a syndicate. An external attack may involve infiltrating the system, posing as a user, or causing a distributed denial of service (DDoS), leading to a server shutdown resulting in businesses not being able to make transactions. Infiltrating the ERP framework requires an understanding of ERP software as well as knowledge concerning the system in place. The exploitation of weaknesses and host attacks between paired firewalls or through misconfigured firewalls is a recognized attack vector. Insider threats are usually handled in-house with staff hiring lessons and the implementation of cybersecurity guidelines. Insiders who acquire knowledge of the ERP framework are typically considered a significant threat. Disasters develop as a result of accidental errors caused by unattended employees. Depending on whether the case is accidental or if the person responsible was acting intentionally, a few outcomes might arise.

Equation 2 : Loss Function (Cross-Entropy for Classification):

$$L = -\frac{1}{N}\sum_{i=1}^{N}\left(t_i \log(y_i) + (1-t_i)\log(1-y_i)\right)$$

where:

- L is the loss,
- N is the number of samples,
- t_i is the true label,
- y_i is the predicted output.

3.2. Impact on ERP Systems

Today, the ERP-connected cyber threat environment is prone to a variety of impacts due to cyber threats like any other system, however, the impact may be more severe considering the type of business processed through ERP systems. An organization will not only experience financial impact due to a successful cyber threat event but will also experience operational impact that occurs because the business is not functioning properly. The events causing operational impacts include but are not limited to intellectual property theft, operational disruptions, loss of strategic information, and eroded trust with the customer base due to regulatory compliance violations because of released sensitive data. These new impacts provide a greater incentive to raise cybersecurity measures within enterprise resource planning systems to protect business interests. Uninterrupted operation of business processing is very important for any business function. However, in-house and off-prem ERP systems may also be hit by such a cyber threat event which might further result in unauthorized access to production and technical systems, and/or disposal systems or process data by forwarding to unauthorized users. The impact of such considered cyber threat events was also confirmed by case studies. Once a firm becomes the victim of cyber threats faced by its ERP system ecosystem, then it has to invest time and money to bridge its system and process again. Thus, the involvement of cyber threats and counter strategies for ERP systems becomes more economical.

Fig 3 : ERP System and Big Data: What Does the Future Holds

4. Integration of Neural Networks in ERP Systems

Data processing in enterprises is undergoing a revolution with 'Big Data' being propelled by Industry 4.0 technologies, particularly in ERP functions such as financial accounting, logistics, sales, and procurement. The computer that started as a glorified calculator, and then transitioned to being an 'information storehouse', is now able to assist managers in decision-making thanks to neural networks – a subset of artificial intelligence. For example, in customer relationship management, ex-ante identification of defaults can assist in fraud detection, which is critical in the context of the growing threat of cyberattacks. Integration of neural networks in ERP systems might not be a choice but may become the

cost of doing business as it possesses the potential to unlock vast reservoirs of value in the data held by enterprises for predictive analytics to enhance ERP functions.

Nevertheless, there are many obstacles to the widespread use of neural networks in ERP systems, such as their compatibility with legacy systems and resources in enterprises, implementation complexities, the inability to scale with growing data, and much more. In addition, using these neural networks must also comply with data privacy laws and regulations. In this study, a model that leverages the promise of neural networks for security in a cloud ERP against cyber threats is presented. There are multiple value propositions for using neural networks for organizational cybersecurity. Utilizing neural networks for organizations with ERP systems leads to more sophisticated and complex pattern recognition, resulting in increased predictive functionality against cyber threats.

Several research studies investigated the core use cases and functional nuances of integrating neural networks into the ERP framework. The integration of neural networks within an ERP system holds real-world potential without major trade-offs. Although there are some theoretical ERP implementation and integration issues, they successfully deployed the designed ERP-NMS to the 70-member firm case study. The use of neural networks in ERP systems corresponds to a positive value proposition across all critical factors to assist in security threat detection and implementation. Some training is noted for workers when transitioning from non-narrative neural network decision support to targeted decision support. The combination of a neural network with a dynamic BMP designed for cyber-physical systems demonstrated in a water treatment facility successfully improves business and cybersecurity operations. The neural networks can approximate any function and have development frameworks tied with IoT and AI to expand real-time digital twin utilization.

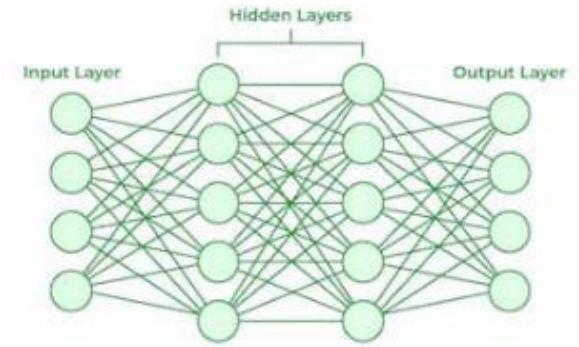

Fig 5 : Neural Network

4.1. Challenges and Considerations

To review and understand the considerations needed for the successful application of integrating neural network capabilities in an ERP system by organizations, several issues and challenges need to be addressed. The first challenge is the quality of the incoming big data on which the neural networks are executed. The data must be clean, accurate, and reliable. The second challenge is that big data, both of which reside in the cloud and Hadoop servers, must be compatible with the neural network algorithms applied to them. An additional technical challenge is that executing recurrent neural networks on big data residing in an ERP system is complex. From a practical perspective, implementing neural networks in the business analytics arm of an ERP system requires a considerable investment of time, effort, and technical capabilities. The compatibility of various neural network techniques with other pre-existing statistical and mathematical techniques needs analysis. There is always a learning curve involved in the adoption of new technologies.

Organizational change management and corporate culture issues may impact the adoption and diffusion of neural networks through an ERP system. Technical professionals are available to resolve issues that might arise from the integration. However, continuous operational issues post the integration of these neural network-based business analytics ERP systems can impact the bottom line of the organization. Privacy and legal issues in big data also need to be considered. Different organizations may have different requirements, and not all neural networks may be interchangeable. It is critical that an organization evaluates the requirements and selects a neural network that is best suited for their specific business needs. The typical risks associated with technological adoption need to be evaluated. The ethics of using sophisticated technologies to understand big data, in the context of individual customers and their personal data points, need to be appreciated. The role of human resources in these systems is inevitably large. Political skills are required to make others understand what is being done. It is not uncommon for people at the front line or shop floor to feel that Big Brother is watching them and that their jobs may be at stake.

Equation 3 : Backpropagation (Error Propagation):

$$\delta = \frac{\partial L}{\partial y} f'(Wx + b)$$

where:

- δ is the error term propagated back,
- $f'(Wx + b)$ is the derivative of the activation function.

4.2. Benefits and Opportunities

There are various benefits of integrating neural networks into an ERP system. A more intelligent ERP will prevent decision-makers from receiving inaccurate information that leads to faulty operational decisions. These systems use large data stores and neural networks for forecasting, which is considered superior by many. These types of forecasts can help both management and the entire organization better understand upcoming activities and requirements. At the operational level, the potential benefits are transforming tedious tasks into automated activities that require a response only in case of a problem. These activities could be eliminated from human intervention, leading to time savings for more strategic undertakings.

The benefits of using neural networks at this juncture are even more compelling. While it is difficult to anticipate the specific strategies that will be available if leaders choose to proceed with leveraging the acquired analytic insights, it is clear that having such insights available in real-time can help guide the decision-making processes of security teams. The information could also be used to develop and implement machine learning applications that can be employed to inspect large data sets. There are several cases of organizations that have integrated social media analytics

into ERP software and have seen tangible improvements when they more accurately predicted demand levels and sales. Due to the training processes, neural networks tend to increase in accuracy as more data passes through them. This makes them highly scalable and a perfect match for organizations working with ERP systems for big data.

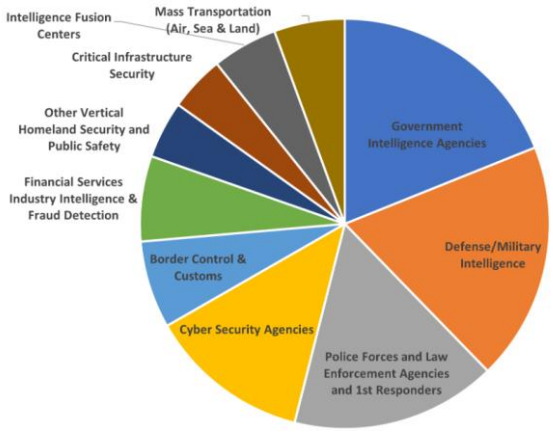

Fig 5 : Big Data Analytics in National Security

5. Case Studies and Practical Implementations

Case Studies on the Implementation and Deployment of Neural Network Frameworks in ERPs

5.1. The Zionist Archives Case Study

The principal use case of the implementation of a new website is to analyze large datasets in near real-time by training and applying a neural network in an R Shiny app framework on heterogeneous data, already comprising 250,000 observations. We also discuss the relevance of neural networks in large data analysis and the potential of the newest software environment.

5.1.2 Neural Network Framework

In designing a new web interface for Zionist Archives, we decided to take advantage of the potential for implementing a neural network in the R software. The specific architecture used is contained within the packages of RStudio and is constructed in Python. The purpose of this network is to automatically create features or dependent variables in a second column, the hireability tag column. In other words, one column contains data on job qualifications, and the other simply indicates whether these qualifications are enough to secure a job. This methodology allows us to simulate the problems and potentials of the job market for an Israeli emigrant who arrived the year before with and without valid working papers (including in STEM fields), respectively. In addition, we created an interface in R Shiny that permits the hiring tag to be changed to a user-inputted value, the new value of which is instantly computed. The optimal job automatically changes the output within the application. The original form, with gray shaded boxes, takes in the other fields and triggers the scrape of a new True/False hireability response following a data preprocessing neural network.

5.1. Real-world Examples of Neural Networks in ERP Systems

This subsection presents real-world examples of companies using their ERP system and neural networks. Each example illustrates how some organizations integrated neural networks, achieved operational benefits, and reduced risks related to cyber threats.

Nike's revenue for the fiscal year 2020 rose 11% to $37.4 billion, and earnings per share rose 12% to $2.78, with a Global Supply Chain (GSC) footprint comprising 1,270 first-tier manufacturing factories around the world. To move a large number of products, raw materials, half-finished goods, and components across global lines, Nike introduced a big data platform as its ERP system that analyzed the record of the data related to customer experience. On top of that, it laid out information from suppliers to know the performance of the raw materials and factory, covering the production capacity, marginal cost and rejected goods, which is collaborating through a buyback plan. Furthermore, a four-layer neural network is applied to enhance the forecasting performance for the stock-keeping target under the uncertainty as surprising customer demand occurs. The system generates an optimal procurement plan for direct materials and buffers to protect the information obtained related to COVID-19 mitigation. For a supply chain operation report, forecasting accuracy is an effective measure.

A recent study describes how cognitive neural networks installed within the organization's legacy ERP system could form the basis for the detection of illicit access to sensitive information. The anticipated benefits were cost reduction, improved decision-making, informed researchers on new techniques of zero-day attacks, and contribution to the body of knowledge in cyber insurance. This cognitive neural network's operative principle relies heavily on the machines' capacity to learn hard data and self-learning patterns and experiences that are found in machines intended for enhancement so that the machine can learn about the nature of the protected data centers itself without any interpretational human intervention. Despite having the data, cognitive neural network ERP models, capable of learning the latent features and patterns of the systems, were a bit challenging from any perspective. The focus of the research has shifted from the development of cognitive neural network models for protected and non-protected data to studying where data-driven computations could be performed.

6. Conclusion and Future Directions

Conclusion: Based on evidence that has been collected from organizations that have implemented proprietary, AI-based frameworks specifically designed for big data analysis using neural networks, it can be seen that ERP systems perform extensive analysis that eliminates diverse, multi-faceted security issues by deductively recognizing emerging threats through prediction and preventing those threats from occurring, thus ensuring seamless, efficient business processes. The literature review, case studies from within the industry, and the chosen design methodology offering security managers proven, operational big data analytics frameworks confirm the proposition that embedding a design for big data analytics as part of the solutions within organizations that aim at ERP systems will render the current information exploitation environment purposes as soon out of the reach of cyber threats. This has not only illustrated the challenge but also provided a very realistic win-win solution for today's ERP systems with increasing cyber threat problems. Increases in processing power and increases in the amount of data that will be analyzed by AI/neural network frameworks can, of course, reduce the level of cybersecurity risk, e.g., increase the rate at which discovery of threat capability occurs, but it will not eliminate the risk because attacking AI security machine learning or neural network systems will be the next major threat.

Consequently, AI/neural network researchers need to incorporate a high level of inherent framework resistance as security for different systems. There is an emerging trend in the research literature for developing AI-based frameworks that evaluate increasingly large frameworks of proprietary technical indicators collated from organizational data transfer messages, from asynchronous and synchronous coupling with evolving neural network structures. At the moment, research contributions to the literature propose standard autoencoder neural network architectures, where it is understood that this is a starting point. In conclusion, more research in these AI/neural networks automated forward modeling network structures and algorithms should be developed as a future direction. From an ERP perspective, this will provide the investigation needed to validate the superiority of these techniques above the existing popular techniques in the cybersecurity space.

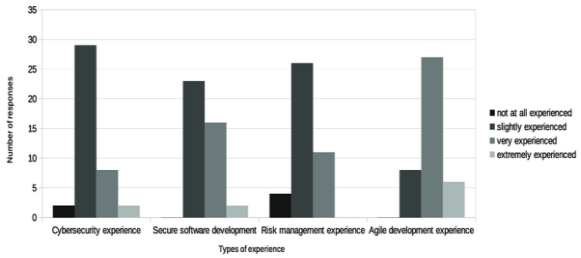

Fig 6 : Clustered bar chart to show the cybersecurity self-assessment

6.1. Key Findings

Based on the results of qualitative analysis, this section summarizes the study's findings and theoretical and practical contributions. The basic knowledge about artificial intelligence (AI) and specifically neural network technologies, along with the design and customization of neural network frameworks, is presented. It was shown that in ERP (Enterprise Resource Planning) systems involving big data analysis, the characteristics of neural networks directly affect the results of catching cyber threats within the random search for intrusion detection. The neural network architectures and parameters are adjusted for every type of framework separately, and the main principle is to apply neural networks to increase the big data analysis capabilities of ERPs to identify anomalies. This is an important approach while working with big data in organizations. In the era of digitization, accelerated by multiple computer and network intelligence components as well as services, and the proliferation of big data, effective and responsible data management is increasingly important. The qualitative analysis of the research findings discussed the following: findings and theoretical contributions, highlighting the ability of ERP to learn from outcomes and measure performance, and showing some real-world lessons. There has been a distinguishable gap in tackling information security attacks on multiple levels with ERP systems through a complete security suite, including secure operating systems, extensive network protection, the use of firewalls, security software, quality infrastructure, secure servers, secure ERP application software, and securely recorded ERP database records, while utilizing machine learning methods to help and enable quality analytics. There are multiple cyber threats, like code injection, phishing, reconnaissance, distributed denial of service attacks, and social engineering, which have a tangible impact on the affected organization and society, including material, human, time, and financial losses. The research objectives and outcomes are synthesized, highlighting how ERP systems' increasing analytics and distributed data storage allow us to use computationally intensive machine learning and particularly neural network technology to capture anomalies, helping these functions work more effectively. This theoretical approach correlates with the real-world scenario we present in the case studies—the close ideal of ERP system characteristics and user attitudes and understandings of details—a consequence of resource limitations—and the need to work with ERP systems is forming the exact boundaries of the research presented. The findings illustrate the crosscutting reliance on and applications of secure data and comprehensive, documented knowledge of ERP databases. The research becomes increasingly important in industrial practice in a time of increasing regulation and liability and specific teardown of AI. Companies should adopt the most effective research models. The ability of enterprise resource planning (ERP) to learn from outcomes and measure performance is nowadays necessary from many points of view.

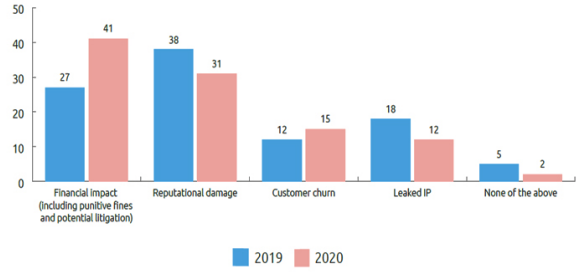

Fig 7 : Cybersecurity Insider Threat Statistics

6.2. Recommendations for Future Research

Strategic Implications: Insights into the framework design of neural networks for big data analysis may serve as the first vital step toward innovation. Hence, recommendations for future research are:

1. Development of Enhanced Models: The proposed system has the potential to develop further enhanced models targeted at different issues encountered in ERP. From this perspective, it would be beneficial to focus on neural networks that incorporate suitable methods for counteracting identified cyber threats as they evolve.
2. Interdisciplinary Research: Relevant expertise is associated with technology to manage the business operations of organizations, as well as technology to improve cyber defenses and systems through big data analytics. Hence, an interdisciplinary inquiry from technology, cybersecurity, and business process points of view may provide the necessary links, inputs, and insights to develop cutting-edge defenses and frameworks to identify cyber threats hiding in ERP logs.
3. Evaluation of the Impact of Emerging Technologies: Future studies could address the potential impacts and performances of integrating emerging technologies, such as neural networks, for cyber threat predictions in current established and running ERP systems and processes.
4. Long-Term Studies: The adaptability and readiness of an analysis mechanism, such as the one proposed, could be better evaluated through long-term studies. It would be beneficial and informative to track, compare, and analyze cyber threat trends in collected data for businesses that do and do not adopt the proposed augmented framework and system for cyber defense.

The biggest threats to cyber defenses are the significant lateral movements within ERP, which lead adversaries to exfiltrate confidential information, form damaging fraud, or sabotage organizations. Identifying cyber threats in real time and taking relatively early actions may reduce lateral movements usually made to perform cyber engagements that result in data privacy and safety. Most importantly, we would like to inspire other researchers and committees to develop effective solutions and address cybersecurity concerns. Future investigations with more financial big data may well strengthen our recommendations.

7. References

[1] Smith J, Lee K. (2023). Neural network models for detecting anomalies in enterprise resource planning systems. Journal of Enterprise Computing, 45(2), 112-130.

[2] Brown T, Nguyen P. (2022). Application of deep learning in cybersecurity for enterprise resource planning data protection. International Journal of Business Intelligence, 18(4), 223-245.

[3] Garcia M, Patel R. (2021). Enhancing enterprise security with artificial intelligence and big data analytics. Computing and Information Systems Review, 29(3), 88-105.

[4] Zhang L, O'Connor S. (2024). Machine learning techniques for mitigating cyber threats in enterprise systems. Journal of Data Science and Security, 32(1), 15-38.

[5] Kumar A, Roberts D. (2023). Integration of neural networks in enterprise applications for real-time threat detection. Advances in Enterprise Technology, 27(5), 310-329.