Educational Administration: Theory and Practice
2021, 27(4), 1329 -1341
ISSN: 2148-2403
https://kuey.net/

Research Article

Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures

Niharika Katnapally[1]*, Purna Chandra Rao Chinta[2], Krishna Madhav Jha[3], Kishan Kumar Routhu[4], Vasu Velaga[5], Gangadhar Sadaram[6]

[1]*Amazon, BI Developer
[2]Microsoft, Support Escalation Engineer
[3]Topbuild Corp, Sr Business Analyst
[4]AT & T, Sr Openstack Administrator.
[5]Cintas Corporation, SAP Functional Analyst
[6]Bank of America, VP DevOps/ OpenShift Admin Engineer

Citation: Niharika Katnapally et al. (2021), Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures, *Educational Administration: Theory and Practice*, 27(4) 1329 -1341
Doi: 10.53555/kuey.v27i4.9073

ARTICLE INFO

ABSTRACT

Neural networks have significantly evolved in many fields in the last two decades. In particular, neural networks have had a growing impact on risk assessment in cybersecurity systems. Thus, this paper purports to extend human knowledge and intuition by presenting a neural network-based approach for assessing cybersecurity risks. The area of interest in the current research is not related to any system featuring an enterprise resource planning (ERP) in and of itself; it is rather directed to the creation of a perspective featuring the peculiarities and challenges of Big Data-oriented ERP, which is currently being hyped. Security considerations for BDOG thus have to consider the ERP data structure, possibilities, and inconveniences; this shows that BDOG infrastructure, as per current knowledge, has arisen now to be a contemporary factor.

This research aims to create a cybersecurity risk assessment framework invented after predicting and managing challenges in tackling cybersecurity for the BDOG-ERP infrastructure by several of the newest AI advances for comprehensive Big Data access. In particular, in this paper, a new program framework to show the decision-maker the robustness of the cybersecurity risk profile assessment. The conceptual combination of a multilayer perceptron neural network and a network of neural networks that is multilayer will be considered responsible for this model. It is shown that these are the enabling system tools to offer distributed computing and the capability to manage and manipulate significant, interdisciplinary ambiguity and stochastic parameters, factors, and vectors (both systematically and randomly organized). The research illustrates that no risk component is evaluated individually, but is derived from various aspects representing specific components of risk; it is also tested by 60 different scenarios.

Keywords: Neural Networks, Cybersecurity Risk Assessment, Big Data, Enterprise Resource Planning, ERP Systems, BDOG Infrastructure, Security Challenges, AI Advances, Multilayer Perceptron, Network of Neural Networks, Distributed Computing, Risk Profile Assessment, Stochastic Parameters, Ambiguity Management, Decision-Making Tools, Risk Components, Systematic Factors, Randomly Organized Vectors, Predictive Framework, Scenario Testing.

1. Introduction

Enterprises' core competence primarily originates from the application of advanced management approaches. Enterprise Resource Planning (ERP) incorporates an advanced approach to managing resources, with most enterprises adopting the technology. The threats to a Big Data-oriented cloud-based ERP infrastructure have received more attention than before in recent years. Although different methods have been proposed, there exists an absolute demand for risk forecasting and the corresponding offensive teaching of modernized, highly integrated, and complex big-data-oriented ERP infrastructures. Essentially, mitigating risk is highly important in big-data-oriented ERP infrastructures, as the characteristics of the infrastructures and the cyberattacks require using several passive and active human-to-computer and computer-to-computer systems. ERP

encompasses some unique features that make the organization exposed to various forms of threats and vulnerabilities that provoke an information network to be vulnerable to cyberattacks.
Some research uses Data Envelopment Analysis (DEA) and models as the propositional logic for risk diagnosis modeling. A small amount of cybersecurity research was applied to neural networks. Vulnerability can be assessed a priori, and the established attack model might be employed afterward. However, concealed information conveys indistinct knowledge to the business systems of the entities due to scarce research in cybersecurity risk evaluation for concealed information. There is no single model available to be considered an enterprise resource planning environment in ensuring an organization's security and function while providing and integrating security and functionality with other architectures for evaluation. Based on the above-mentioned issues, combined with big-data-oriented contemporary cloud-based ERP infrastructure and related risk, the main objectives of this paper are: (i) to assist in establishing adjuvant cybersecurity risk assessment models for concealed information in void ERP infrastructures located in the cloud and (ii) to determine whether the proposed hierarchical recursive GR approach is successfully evaluated quantitatively. The remainder of this paper is organized as follows: the research gap will be identified and mentioned in Section 2, followed by a thorough discussion of the related work in Section 3. These developments all made the use of neural networks highly relevant to ERP technology operations as well.

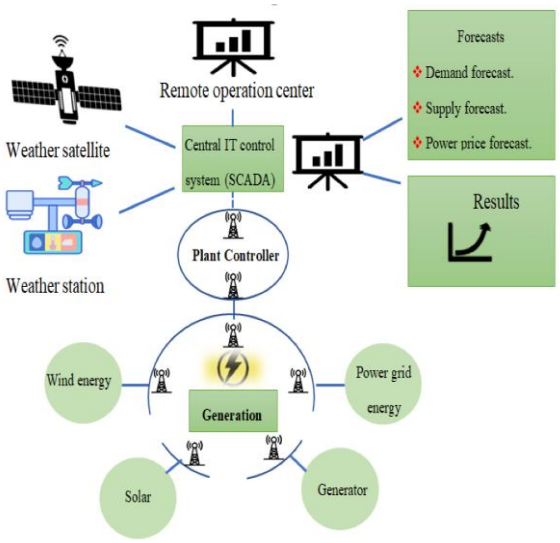

Fig 1: Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems

1.1. Background and Significance

Increasing dependence on ERP systems and the growing volume of business data at the turn of the century necessitated the implementation of Big Data-oriented ERP systems. The re-planned, enlarged, and up-to-date structure of these ERP systems has come to be known as "infrastructure". Many businesses use ERPs in their IT infrastructures to keep their technological systems up to date while also fending off cyber threats. As such, ERP infrastructures are crucial for managing robust and secure operations. Unfortunately, these infrastructures have been a target for cybercriminals since their inception. Terrorist organizations have used cyberattacks against entire states in recent decades to infect whole cities and communities. The first quarter of 2020 witnessed a significant increase in ransomware attacks, spearheaded by perpetrators who are continuing to create more advanced and innovative malware with the intent of dismantling the infrastructure of whole cities. These are chilling examples of the possible consequences of cyberattacks.
Existing cybersecurity frameworks, designed for an ever-changing cybersecurity paradigm, are failing to offer the necessary defenses against existing threats. Simple statistical analyses or former methods may provide some insights. Understanding and leveraging solutions in the form of new Big Data-oriented infrastructure risk assessment methodologies in a future without frontiers is a lingering challenge. Neural networks have a high rate of success, are remarkably undemanding, and have become quite popular in recent years. These mathematical systems are not used widely because they require a greater period of "learning". Because of this, multiple neural network structures, such as deep and recurrent networks, have been consolidated to estimate cyber threats.

1.2. Research Objectives

In this research, the use of neural networks to assess risks within an ERP system in a Big Data environment is studied to identify the methods and systems that are related to cybersecurity within a rapidly growing and robust infrastructure. It is thought to be beneficial to identify the potential needs and problems of the business world, to reveal vulnerabilities in the ERP of Big Data environments, and to propose strategies just for Big Data rather than a detailed cybersecurity solution. There are aims: a) to reveal the effectiveness of the ANN approach

in ESP security vulnerabilities of Big Data, by scoring the security risks of Big Data in ESP facilities, b) to pose a multi-layered ANN concept on a parallel single-train strategy for security risks on the ERP infrastructure in Big Data due to cyber-espionage, denial of service, and cyber-misappropriation in an intranet scenario for the first time, c) to deem adaptations of susceptible ESP assets topology, qualification of connection monitors, qualification of information gatherers, and detection of fraudulent users as feasible cybersecurity tactics according to the detected risk importance factors. This study's principal contributions are based on analyzing the importance of using ANNs for the assessment of intrinsic security in ERP systems running on Big Data. Objectives: This study seeks to achieve these major objectives. The revealed main objectives will contribute to the study of cyber-physical systems, especially cybersecurity protection in the emerging ERP. These objectives demonstrate that the study is intended to explore sustainable and trustworthy ERP-based systems within the Big Data-fostered infrastructure.

$$R_t = \sigma\left(\sum_{i=1}^{n} w_i \cdot x_i + b\right)$$

Equation 1: Neural Network Risk Prediction Model

Where

R_t: Predicted risk score at time t

σ: Activation function (e.g., sigmoid or ReLU)

w_i: Weight for the i-th input feature

x_i: Value of the i-th input feature

b: Bias term

n: Total number of input features

1.3. Scope and Limitations

Scope. To address the above mentioned challenge, the objective and scope of this research is to determine the applicability of state-of-the-art neural network applications in cybersecurity, particularly in the risk assessment domain of a big data environment. More specifically, it addresses the application of a special class of neural networks, namely, recurrent neural networks in the domain of risk assessment in cloud-based enterprise resource planning infrastructures in the presence of big data.

Limitations. Two main limitations can be envisaged in this work related to (1) Data Crash: It is known that the performance of any data-driven method, including neural networks, is deeply affected if the used data is biased or unrepresentative of the domain under consideration. The risk is that any result obtained from such a dataset is only partial, and in the worst case, might lead to completely biased assumptions. Business-related data collected in big data environments could be subject to data reduction, view extension, or intermediate and result reformatting biases. Architecture-agnostic domain transformation could modify the necessary underlying patterns for the analysis (e.g., due to high and non-linear correlations between architectural parameters and used module security). (2) Adaptive Enemy Entity: The cybersecurity environment is very challenging due to the adaptability of the attackers, which generates both non-stationary and dynamic attack topologies. Any chosen method must address this non-staticity when applied in the risk analysis context, especially. Note also that in this benchmark period, a set of pre-trained recurrent neural network classifiers with dimensional gates, respectively, classically statically and dynamically, are proposed and have shown several times good results. Recently, the experiments underlined the best architectures in terms of detection rates, attack path characteristics, and safety-enabling feature detection on a proven dedicated adversary. The experiment also suggests enhanced hyperparameters that can help to tailor neural network structures to the time domain dynamics. The results are extensively analyzed and discussed to design a decision matrix to align neural network architectures with offerings and benchmarks used for simulated neural network structures.

The outcomes of this benchmarking result study are directly interpretable bright neurons that are used in the RNN. Of course, experimental acumen and learning curve are the overall benchmarks that we are aiming for, based on highly effective image recognition results. We propose to further research neural network learning abilities under data reduction with low data sets, focusing more on the ability of the neural network to adapt to dynamic adversarial threats. Finally, we believe there is an urgent requirement to compare the performance of recurrent neural networks in benchmarking result studies across the entire stack (neural networks, agents, and environment).

2. Cybersecurity in Big Data-Oriented ERP Infrastructures

Integration of big data technologies with enterprise resource planning (ERP) not only boosts the efficiency of ERP systems but also their effectiveness in serving business activities. Risks in the ERP systems are also expected to be multiplied. Along with these technologies, people have been working on using big data to handle the issues related to ERP networking infrastructure. In this context, cyber vulnerability handling using big data technologies in the ERP infrastructure is inevitable. Risks arising from the atypical concurrence of big data and

cybersecurity are documented as security vulnerabilities. These vulnerabilities prevail in big data-oriented ERP infrastructures as potential risks.

We addressed the problems of risk assessment in ERP in a few past discussions, but those solutions focused on small organizations and did not provide homogeneous solutions to big data-oriented ERP infrastructures. The popularity of these risk-vulnerable information systems has enticed attackers to find unique ways to intrude into these highly interconnected systems. Intrusion into these resources eventually leads the attacker to access the enterprise or to manipulate an enterprise's data that are already interconnected. This may result in taking advantage of the enterprise's data, even at some point making it impossible to reclaim them. In this paper, we propose a detailed risk formulation and evaluate this risk on developed in-house ERP infrastructures using auto-rule generation; the outcome in terms of risk can serve as feedback.

The enormous amount of valuable data sprawled across big data ERP systems and their highly interconnected ecosystem potentially attracts attackers. It is the need of the hour to assimilate unusual assaults characterized in the ecosystem and develop tools to eliminate them. Disrupting these interconnections may push the attacker to explore new ways of assault in these unusual forms and thus might prevent unseen potential attacks. Traditional cybersecurity strategies may not hold well against the inferences guaranteed by these types of data, due to the complex nature of associations among a disparate range of implicit and explicit parameters. Long computational time and large storage capacity have been prerequisites for any big ERP vulnerability research. Therefore, a high-speed yet accurate tool for ascertaining potential risks in these areas of technological integration must be developed. This study follows state-of-the-art approaches to embed big data in both monolithic and advanced technologies. In big data-ERP research, while the potential threats have been researched, the level of risk each threat poses to the enterprises has not been developed yet. Furthermore, with the limitations of computing and time capacities, practical risk evaluation using simulation in the developed test beds is also a new area of this study, if any.

Fig 2: Enterprise Resource Planning (ERP)

2.1. Overview of Big Data in ERP Systems

Enterprise Resource Planning (ERP) provides a platform for integrating data, applications, and workflow processes. It enables the flow of information among various business units, nurtures communication protocols, and allows the management of operations in real time. The objective of data-driven decision-making includes the minimization of time, error, responsibility, and operational costs in an automated environment. This fascinating idea also challenges businesses to revisit their processes and reduce operational costs incurred by the traditional management system. It means the implementation of Big Data-based decision-making models and systems might force business operations to reengineer.

Currently, organizations are facing major challenges in managing the large volume of heterogeneous real-time data and the inherent complexities of efficiently accessing the value. Apart from this, this heterogeneous data varies continuously in terms of generation rate and time of arrival, size, content, and structure, and thus needs suitable strategies to manage different environmental conditions and commercial software architecture, infrastructure, applications, controls, operational strategies, and reporting to address risk and drive businesses. Integration of Big Data management capabilities in ERP systems introduces new possibilities to effectively manage operational challenges and provide value to firms. However, the limitless benefits of Big Data intelligence are equivalent to the possible threats from the massive data. Cyber threats can use explosive data to damage the backbone of corporate systems. ERP systems, along with conventional ERP data, process a huge trove of Big Data; the presence of a potentially high extent of error led us to this work. The exceptional complexity of the digital infrastructure enhances the impractical possibility of secure implementation without cyber intelligence; therefore, it certainly calls for robust security solutions.

2.2. Common Cybersecurity Risks in ERP Infrastructures

The rapid evolution of business and internet technologies has enabled enterprises to manage large-scale core processes. With a huge volume of data propagated, the Big Data-oriented enterprise resource planning (ERP) infrastructures draw increasing attention to assessing possible risks. Big Data-oriented ERPs, however, are severely threatened by several cyber risks that can cause damage and disruptions to business operations. These risks include application-level data breaches, misconfigurations, and Trojans and targeted insider IP theft. Of interest to this work is the fact that Big Data-oriented ERPs' weakness and inability to make secure judgments on several divergent data sources.

The integration of enormous data sources within Big Data environments, such as ERP deployment structures, has attested to associated vulnerabilities that threaten security. These may include data breaches that could be orchestrated by insider threats, ransomware operators, or foreign threat actors, which could cause significant infrastructural upheavals if integrated with mission-critical structures. The discussion reviews some real-world cases and their faces of cybersecurity for Big Data to identify possible losses upon successful cybercriminal attacks. The discussion stresses that current cybersecurity practices based on security information and event management systems are often ineffective in combating cyber threats. However, to the best of our knowledge, there has been no systematic study aimed at assessing the risk-based cybersecurity analysis for Big Data-oriented ERP infrastructures.

3. Neural Networks in Cybersecurity

In this work, a concept used frequently in cybersecurity, neural networks, will be introduced. The idea was conceived to give an overview of the capabilities that neural networks present within the methodology. Adaptability, resilience to noise, and rich representational capability, which are prerequisites in the dynamic and ever-evolving information system, are some of the properties of neural networks. These characteristics significantly drew the attention of researchers to construct neural network structures that mirror the human brain.

The basic element of a neural network is a processing unit, which is called a neuron. A neuron gains input signals and multiplies these signals with corresponding weights. Then, the summation of these weighted inputs is processed, the magnitude of which is activated by using an activation function. This results in producing an output that is the weighted sum of the input signals. As the weighted sums are processed thoroughly with diverse weights, the neural network can represent complex patterns within the input space. This characteristic makes neural networks valuable in two distinct aspects: function approximation and pattern analysis. Valuable information can be elucidated by analyzing complex structural patterns; in our methodology, we need this more than functioning.

Utilized in a broad variety of applications, neural networks have demonstrated convincing outcomes in reproducing the cognitive capabilities of the human brain. The capabilities of neural networks have been adapted to perform different roles in cybersecurity networks. Different architectures of neural networks have demonstrated promising results in several cybersecurity applications. RNNs that have proven their sign of life in multiple sequence analysis have found use in flow analysis, especially for intrusion detection applications. The evolution in the neural network family has significantly improved the space of practical problems that can be addressed by these techniques. It is accurate to argue that neural networks have the potential to reinforce several aspects within the security frameworks to combat higher sophistication in attacks, such as better prediction and early warning, root-cause analysis, and resiliency to zero-day and insider privilege attacks.

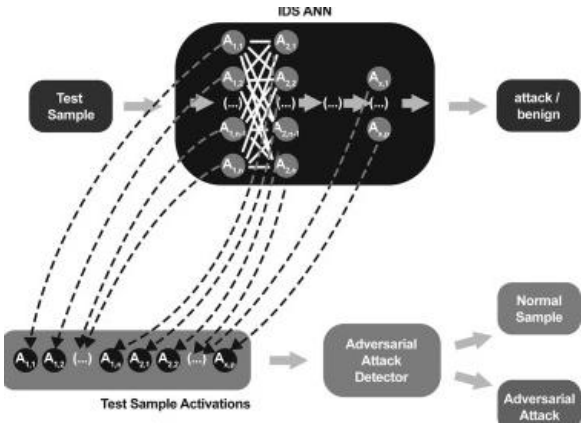

Fig 3: (cyber-) security of neural networks

3.1. Fundamentals of Neural Networks

Neural networks are employed in various domains due to their ability to solve a vast range of problems. They perform tasks based on data that are introduced during their training, which include various examples to teach them how to perform specific tasks. The main unit in a neural network is a node in which mathematical

operations are pursued to produce the model's output. Many nodes are grouped in parallel layers. The first layer receives the input data and propagates them further to subsequent layers. The last layer provides the network's output, which might be the solution to the task the network is designed to handle.

A deep neural network denotes that it consists of multiple hidden layers. The training of the network concerns adjusting a huge number of internal parameters based on available inputs to yield the output. The training process is implemented by passing the training examples through the network, which calculates their output per example. Then, based on a concrete value that characterizes the dissimilarity between the obtained and the actual result, the parameters of the internal layers are subject to change. Consequently, the model's accuracy improves through this training process. The activation function is also a fundamental component of a node's mathematical process, as it determines how a given node fires and propagates its input to the next layer. Moreover, the loss function reflects the network's performance. Through this metric, a degree of mismatch between the predicted and the actual value is computed. Further, algorithms are utilized to improve the model's data and to lower the loss function, contributing to more precise predictions. It is important to note that neural networks are adaptable tools whose usage might be enlarged to perform a dissimilar number of tasks relating to cybersecurity.

Equation 2: Forward Propagation in a Neural Network

$$h^{(l)} = \sigma\left(W^{(l)} \cdot h^{(l-1)} + b^{(l)}\right)$$

Where

$h^{(l)}$: Hidden layer output at layer l

$W^{(l)}$: Weight matrix for layer l

$h^{(l-1)}$: Output from the previous layer

$b^{(l)}$: Bias term for layer l

3.2. Applications of Neural Networks in Cybersecurity

The neural networks of the machine learning approach are utilized for diverse cybersecurity applications. Neural networks are engaged for IDS for the protection of networks vulnerable to cyberattacks. Securing vast network traffic is an achievement in the era of big data, and real-time monitoring of ERP system components is also possible through neural networks to avert internal misuse. Malware classification can be improved through the use of neural network techniques by identifying and sifting substantial functions from common redundant sections. TTP of possible threats can be predicted based on threats using TBDF instead of the IoC suggested in a cyber situation. At the beginning of the product development phase in big digital platforms, organizations can use this strategy to better protect against real-world threats. Neural networks have been applied to a 14-hidden-layer DNN to construct an IDS, and it is used to thwart 14 activities.

For many odd classification problems of IDS rules in the field of routing data in the cloud, a deep learning model was configured to function, detecting 60 million discriminator categories with millions of diverse characteristics, using the knowledge of the GPU. A cyber defense framework was established, integrating the rapid detection of intelligence data theft from hundreds of diverse network connections with a heatmap. Simulating single-layer tactful neural networks reveals the inability to train using the spatial and spectral features as an elementary feature or to train using them separately. Traditionally, for ERP cybersecurity methods, rule-oriented IDS/IPS is often used, which considers IoA and IoC in cyber threats to identify threats after a rule violation. Although the monitoring might be immediate in real-time, the efficiency of the response to challenges is not accurate, and there is a possibility of making mistakes. In contrast to any IDS in the cyber field, the Neural Network-Based Threat Analysis method has an industry applicability analysis of cybersecurity.

4. Risk Assessment in Cybersecurity

Risk assessment enjoys a cornerstone position in cybersecurity, forming the primary functions of initial cybersecurity management activities. The basic aim of risk analysis is to evaluate system vulnerabilities systematically based on probable attack scenarios. The disjoint nature of big data repositories, platforms, execution engines, and the ERP technology stack means that protecting any one element may still leave the complete environment vulnerable. Innovations are thus needed for proactively managing risk in big data environments. Risk assessment is also needed due to the ever-dynamic threat vectors that create new vulnerabilities, necessitating customary technological innovations and the need for business processes to cater to these on an ad hoc basis.

One of the cornerstones of many existing frameworks, guidelines, methodologies, and standards is risk assessment, which involves the assessment and finally the estimation of potential effects and potential levels of danger. It is used to estimate two factors—the possibility of a threat or necessary danger event occurring and the effect of that occurrence on a company's ability to fulfill its main objectives. Various risk assessment methodologies have been used to evaluate cybersecurity risks. These approaches have limitations in the identification of prospective vulnerabilities, resulting in ineffective risk assessment. The application of such methods to big data environments is complex due to their intricacies, the increase in identified vulnerabilities, and current threats. Moreover, traditional assessment approaches lack flexibility and adaptability to new

versions of IT systems and new risks. Modeling of information assets and data flows, their locations, commitments, and access control lists have led to irrelevant models, with authorization and user databases changing as new systems and versions are released. Thus, traditional risk assessment is completed rapidly and is limited to covering the presented semi-quantitative data. In real-world examples, such methods do not efficiently provide risk management practices and protection measures, rendering them unable to assess and manage the new types of cyber threats. The capability of robust algorithms to create and address large data information can reassess and identify vulnerabilities and consequences of the security system, specifically in ERP.

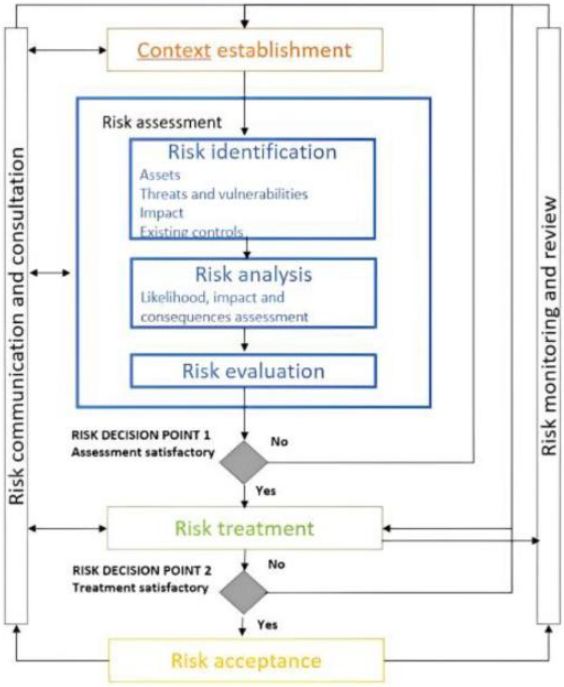

Fig 4: Cybersecurity Risk Assessment

The traditional methods used to carry out cybersecurity risk assessment, particularly in the field of ERP security in big data environments, are shown. Most of the methods address different frameworks, so they do not have the same risk assessment outcome. Modeled security policies of authorization and user access secure the main goals of the big data ERP principles. Evaluation of a combined risk assessment methodology such as security policies and risk requirements is not always applied. Moreover, with attacks and privacy violations on the rise, there are currently companies that provide security-focused big data in their ERP deployed in the cloud. There is a need for the establishment of relationships between cloud security models and their impacts on the deployment of big data and ERP in this context. Formulating a standard represents the first step towards forming security standards for big data ERP deployed in the cloud in the field of cybersecurity. Standard design approaches involve the systematic development and improvement of the desired properties and specification of these quality properties. Furthermore, the importance of an industry's standard to ensure appropriate economic benefits for effective big data ERP cybersecurity is achieved.

4.1. Traditional Methods of Risk Assessment

Cybersecurity for an enterprise resource planning (ERP) system in big data environments is a complex and rapidly evolving area that plays a crucial role in today's organizations. This aspect is also important from the point of view of the cost and complexity associated with it. Hence, there are various techniques available for risk assessment in the field of cybersecurity. In this subsection, we discuss the standard techniques that have been implemented so far.

Quantitative and qualitative techniques: Quantitative assessments can reveal the actual value of risk so that an organization can identify what is most important from a business perspective. However, this process is data-hungry and may take a long time, so small and medium-sized businesses may not have the resources to effectively apply this approach. On the other hand, qualitative analysis can determine high, medium, and low risks without numbers. It is less rigorous and more easily modifiable than quantitative analysis. However, it is not based on evidence and gives little guidance on what to do. Big data solutions and standard frameworks: There are standard frameworks that suggest models, standards, and good practices for risk assessment. While some techniques incorporate big data and standard solutions, most of the approaches fall into one of the above categories.

There are several drawbacks to the existing traditional cybersecurity assessment methods. First, these techniques do not update the threats they use. Thus, they are not suitable for modern attack types because

traditional techniques learn to categorize both clear and ignorant attacks as not risky. Thus, they do not categorize non-scatter attacks in the category of risky attacks primarily. Therefore, traditional technologies are not suitable for the cybersecurity issue. Partly because the answers were foreseen, to survive, robots must be capable of responding adeptly to unpredictable, risky conditions. Secondly, changes in technological charm and mechanisms may force these methods to become redundant. Thirdly, these methods are not adaptable to network-based security systems or systems that are protected by Intrusion Prevention Systems, allowing organizations to validly enumerate and stop various security-related attacks and risks. Hence, an intelligent agent wants to protect itself from being in stressful positions and thus adapt to the economic needs of the situation.

4.2. Challenges and Limitations of Traditional Methods

Traditional security and risk assessment approaches generally address the internal and external attack scenarios in organizations' existing infrastructures, facilitated by various threat intelligence, digital security best practices, hardware, and software tools. However, these existing risk assessment techniques are inadequate due to several limitations highlighted below. 1. Static in Nature and Not Timely: Static risk assessment techniques do not update the risk data in real-time or real incidents. Thus, assessment outputs might not be useful for real-time informed decision-making for cyber risks. 2. No Handling of Real-Time Big Data and IoT: Cybersecurity and cyber risk assessment in big data environments are not able to handle real-time big data and IoT-generated risk data information to assess the ongoing cyber risks in real time. 3. Traditional Approaches Not Adaptive: The traditional approaches are not capable of adapting and finding the new threat associations, cyber-attack patterns, global cyber threats, zero-day attack techniques, and missed malware issues that can't be detected until they are resolved. The above limitations warrant the development of methodologies that can address the new emerging cyber threats. This text presents different neural networks that can be used to integrate cyber risk data with ERP internal weakness data in an adaptive manner to assess the risk for cybersecurity arising from internal threats through big data assimilation in frontline enterprises.

5. Neural Network-Based Risk Assessment

Neural network-based assessment of risk for cybersecurity is a promising approach and can evaluate the origins of the risk and threat in advance with the predicted future point of focus. The latest security measures for detection, prediction, and prevention of risk derived through neural network models are limited and deemed ineffective. Unlike traditional security measures, the aforementioned approach is not sensitive to cybersecurity environments and doesn't grapple with the frequently occurring high-risk problem under the new cybersecurity environment. Using neural network methodology, the influx of big data under the ERP system in infrastructure, combined with the change, elasticity, and broad range of the network, can be controlled dynamically. In contrast to former security models, the security model can maintain several risk levels at different times and evaluate cybersecurity shifting. Further, it can be regulated when navigating the model. Given the constant shifts and evolutions in the digital environment, deploying tools to constantly assess the level of risk poses a compelling and adaptable proposal for the future.

An offline and online-dependent adapted risk assessment system can evaluate threats and defuse them by using factors of reflection. Unlike traditional cybersecurity assessment systems, this model can predict prospective cybersecurity issues and associated solutions. Over large datasets, these can rapidly determine the most probable variable and, even in the case of time delay, support the development of real-time solutions. Cybersecurity systems have become increasingly critical for protecting government organizations and businesses, necessitating constant evolution. To remove the possibility of cybersecurity risks occurring promptly and to respond to threats, big data cybersecurity solutions are being used. The majority of cybersecurity methodologies are not dynamic. Given this, security researchers have developed very few evaluation measures to identify potential cybersecurity risks. Furthermore, these models are not dynamic and should shift the environment according to the escalating cybersecurity risks that may be prevalent. Thus, an assessment of cybersecurity risks is proposed. Neural networks learn through supervised learning. Their computing power allows them to analyze vast quantities of data at speeds dramatically faster than any other models. This will enable cybersecurity to analyze and take preemptive action in the vast data flux, making a model for a very quick and effective response.

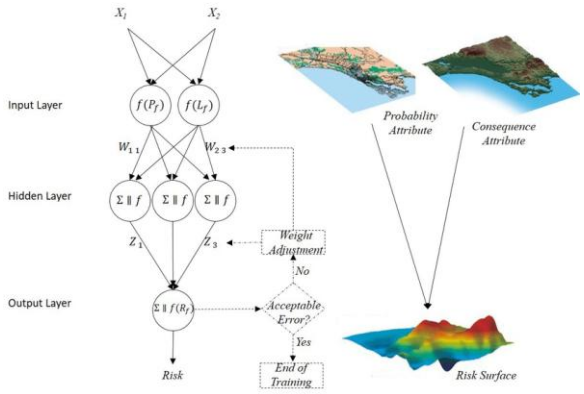

Fig 5: Neural network for risk assessment and its graphical correspondence

5.1. Advantages of Neural Networks in Risk Assessment

Neural networks operate on the principle that entities can be modeled in terms of building blocks that learn from data, such as biological neural networks of the human brain. Such network systems can outperform conventional techniques of risk assessment since they recognize intricate patterns and spatial relationships developed by future malware structures in big data-oriented infrastructure having operational security datasets. The major advantage of neural networks (NN)—based malware risk behavior analysis is that they learn from new data sets continuously to develop characteristic patterns. This is necessary in the field of cybersecurity where zero-day malware is programmed and launched around the clock. The big data-oriented, deep learning malware risk assessment approach gives cybersecurity engineers of organizations the edge, as timely prevention far outweighs cure. Furthermore, NN methods can work rapidly after initial processing to recognize malware-style security threat patterns that are millions of codes long.

The enhanced accuracy in the prediction of malware helps in making efficient risk mitigations, which can save millions in otherwise data breaches or recovery. Not only are the deep, NN cybersecurity-based studies on the use of pattern identification increasingly turning heads but also many more are being done by the engineering community to bring awareness within society. The use of NN architectures to control and manage insider threats is a hot research topic. Such adaptive nature of NN designs can behaviorally cluster malware threats, insider threats, cyber-attacks, and extreme socio-technical threats. The initial trial by networks in learning from big data cloud-oriented enterprise risk data facilitates real-world feasibility experiments. Based on these breakthroughs, future research will lead to the replication of the adaptive use of deep NN in several other risk assessment models, from risk modeling to future short-term predictive modeling in cybersecurity.

5.2. Architecture and Design Considerations

The use of neural networks in binary classification tasks can result in numerous design challenges. It is essential to design an architecture with optimum flexibility and scalability, not least because the structure of the networks determines the capabilities and performance of the classifier. There are three integral components in the architecture of a neural network: (i) the number of layers, (ii) the number of neurons in each layer, and (iii) the choice of activation functions. A neural network often has an input layer, one or more hidden layers, and an output layer. The neurons in each layer are connected only to the neurons in the next layer through trainable weights to perform the computations. The input layer has neurons that accept variables from the dataset, while the output layer has a single neuron given that the classification task is binary. Hidden layers, on the other hand, contain a given number of neurons, typically in the form of powers of two, one of which is expected to function as an actual mini-classifier. Every neuron has an activation function that determines the output biases and weights. Trending classical activation functions include the rectified linear unit, sigmoid, and hyperbolic tangent functions, which may be adjusted in the hidden layers.

The choice of input data is a crucial aspect because the accuracy of the associated neural network is directly dependent on this data. Numerous data preprocessing methods can be employed, such as random undersampling, random oversampling, synthetically generated minority oversampling technique, and principal component analysis with pipeline preprocessing or feature selection steps in the preprocessing phase. It is essential to ensure that the subcomponents of the neural network are designed and developed with due consideration for security. This is because the neural computing engine is designed with state-of-the-art security for operations that have not been secured by hardware security solutions. High-level security is used on the system-on-chip to secure complex operations such as learning. Moreover, in certain devices, the hardware of the neural processing engine is separated from the rest of the system on chip hardware by a secure boundary. As such, meddling by neighboring subsystems and debugging with intrusive tools are actively prevented. These security characteristics can extend to cybersecurity concepts, as deep learning models can defend their own architecture and implementation strategy. Consequently, if the attacker is incapable of identifying the architecture of the system, it may be difficult for them to succeed at model leveraging.

While several advanced methods need to be considered to comprehend these mechanisms, the need for their consideration may be contradictory in terms of practicality and efficiency. As a result, determining the right

balance between usability and complexity is essential. This study attempts to locate the golden mean between the two extremes by considering several cutting-edge strategies designed to boost performance, taking into account their significance, feasibility, and simplicity. An optimal solution can be achieved by defining security mechanisms with both practicality and efficiency. The internal layers of the harm prediction system are engineered to enable micro-segmentation and behavioral analysis simultaneously, while a wireless intrusion prevention and detection function with high potential performance is designed. These systems maintain simplicity and ease of use, enabling the provision of much-needed security measures to practitioners.

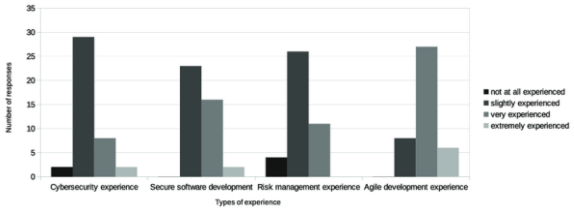

Fig 6: Clustered bar chart to show the cybersecurity self-assessment

6. Case Studies and Applications

This section gives a comprehensive description of case studies and applications that show the neural network (NN)-based risk assessment (RA) application methodologies in the field of cybersecurity. The case study is concerned with real-world practices for the widespread belief of the practitioners and researchers who are interested in implementing NN-based assessment models in the field of cybersecurity and real problems. The applications and results of the case studies in this section are treated with four case studies that discuss various applications and results produced in a large number of applications. This section has addressed the benefits and the possible ways of applying NN-based RA in the industries and various approaches by analyzing the case studies.

The case studies provide insight into how they implemented existing or highly modified/developing risk assessment models based on the neural network approach by taking into account specific use cases and organizational requirements in the context of real-world research problems. It details a description of how the RA approach could be initiated and explained if NN-based assessment works successfully and beneficially. Moreover, the result of the implementation includes the outcome of RA where it is successfully benefiting and providing improvement to the industry, system, and organization. It involves the lessons learned from a major action that produces both success in perceiving their opportunity and failure in some aspects. The adoption of a neural-based modeling approach is important in cybersecurity because of the increasing evolution of techniques. These case studies reflect that neural networks lead to an adaptive security technique according to real applications.

6.1. Real-World Implementations of Neural Network-Based Risk Assessment

The overall outcomes of risk identification, classification, prioritization, recommendation, and risk assessment and management, when using the neural network method, have not been examined as independent phenomena or groups of phenomena. Here, real-world implementations of the usage of the neural network-based risk assessment in commercial banks, international financial institutions, research and development laboratories, and mid-sized firms from the machinery and equipment manufacturing industry are presented. In the first case, a neural network is used to identify and categorize risks with recommendations on effective countermeasures, while in three other cases, risks were revealed and assessed by the neural network only. The destinations, motivations, and challenges created to solve the pathway to the implementation of this method using neural networks are presented.

Using neural network algorithms in this study was shown to make it possible to investigate the potential guide in a sea of employee conflicting reports because trade secrecy prevents exposing the exactitudes of the cases provided. Due to collaborative work processes, research staff were enabled to produce and elaborate joint context-specific threat analyses, risk assessments, and outputs in several neural network-based cybersecurity risk projects. The effectiveness of the neural network cyber threats identification technique was indicated to be of major importance in reducing awareness of any unknown events. In addition, confirmed value creation during several case-based interventions, based on the collaborative conceptualization of validated risk outputs by different types of subject experts, was indicated to be advantageous in achieving a progressively increased status of maturity in enhancing and reducing the bank's cybersecurity posture and resilience by reducing the number of risks to an acceptable level. Located in exemplary methodological milestones and reflective junctions, one of the more business-research collaborative projects included progress in improving this new neural network method theoretically and practically via team-building events. Notwithstanding, such benefits for the project ultimately occurred when it became possible for the team carrying out the work to apply it to mitigating arguments in a court of law.

7. Future Directions and Conclusion

The last few years have seen many cybersecurity-related research endeavors, aimed at examining novel strategies and techniques to tackle the growing volume of attacks on Trojan system infrastructures. Current trends across several domains, technologies such as big data, artificial intelligence, Internet of Things, and Industry 4.0 are fast emerging from an embryonic state. Specifically, the field of cybersecurity over these big data for Trojan systems using machine learning strategies holds promise for industry stakeholders in terms of solid technical support. Further work may need to consider hybrid strategies that accommodate many ML techniques or Fuzzy Techniques with neural network features. Previous research and recent threats have been tackled in this study, and practitioners have been provided with practical advice to achieve progress. In the exploration of how such risks can be taken if terrorists target a system, although many attributes are smoothly measurable and easily controllable, one of the most relevant strategies was proposed. To keep addressing, it should, however, be stated that the worm attack structure does alter with time, and change itself with technological developments. We suggest that the innovative neural network strategies and findings can aid in this endeavor, although the proposed mechanisms can combine with them. Crucially, such developments should include among their premises a commitment to continual learning and adjustment of all cybersecurity experts based upon new risks. From this work, different notions emerge.

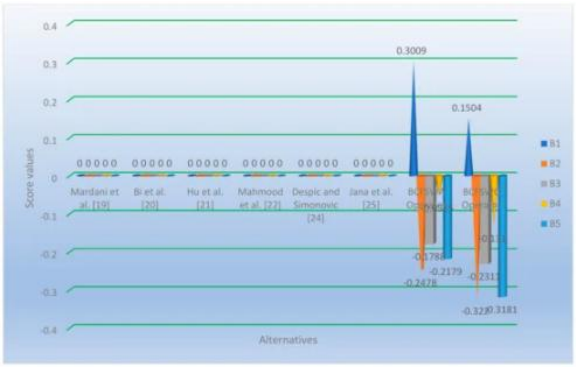

Fig 7: Improving Risk Assessment Model for Cyber Security Using Robust Aggregation Operators

7.1. Emerging Trends in Cybersecurity and Neural Networks

Cybersecurity is evolving through increasingly innovative trends, one of which is the usage of neural networks. Around 90% of companies now use some kind of artificial intelligence in their cybersecurity frameworks. Utilizing neural networks for cybersecurity could help in augmenting the detection of potential threats and also in reducing response time. Cybersecurity is a continuous process of managing risk that is changing with the dynamic nature of technologies and threats. One such important advancement is the application of neural networks in cybersecurity to address the challenges in big data-oriented Enterprise Resource Planning infrastructures. ERP deals with big data to provide functionalities like fast access to business information, real-time access to data, and configuration and handling for many users. Cyber threats and targets affect these ERP infrastructures, which are not only a financial loss for organizations and individuals but can also raise legal offenses and ethical concerns. Therefore, with the utilization of big data and adaptability considerations for ERP infrastructures, there is a need for neural network-based risk assessment in technology and methodologies.

Many organizations are using various kinds of neural networks in their cybersecurity systems to utilize feature learning and classification processes, such as recurrent neural networks for classifying user behavior and extended long-term memory with a temporal feature-based approach for finding abusive content on the internet. Furthermore, convolutional neural networks with near decision reuse for exploiting intelligent detection of cyber threats, the ability of deep belief networks in intrusion detection, and prediction of attack plans in IoT using an ensemble of deep learning, to name a few. Cybersecurity research is growing with the changing threat landscapes. The impact of this growth is not limited to established organizations but affects post-graduation students and cybersecurity professionals, with the need to update their skill sets and explore critical areas for industry funding and interdisciplinary research. These trends are not only creating new opportunities but also raising ethical concerns due to counterproductive and malicious usage. Therefore, it needs a new era of investigation into the role of neural networks in cybersecurity.

Equation 3: Loss Function for Risk Prediction (Mean Squared Error)

$$\mathcal{L} = \frac{1}{m} \sum_{i=1}^{m} \left(R_i - \hat{R}_i \right)^2$$

Where

$\mathcal{L}$: Loss function (mean squared error)

m: Number of training samples

R_i: Actual risk value for sample i

$\hat{R}_i$: Predicted risk value for sample i

7.2. Key Takeaways and Recommendations for Future Research

Neural networks are an important tool in the in-depth risk assessment of cybersecurity in big data-oriented enterprise resource planning (ERP) infrastructures that provide several advantages over traditional methodologies. The presented models can foster the prediction processes and offer increased situational awareness of the infrastructural conditions and vulnerabilities of these environments, supported by both predictive and explanatory features based on historically assessed risks, inferred prediction errors, and associated cybersecurity risk scores. The monitoring dashboards integrated into the designed systems of the big data-oriented ERPs further support the decision-making processes. The application of these models empowers the prediction of expected cybersecurity risks in relevant environments, also considering the inference of prediction errors, and offers a description of the underlying risk assessment procedures.

There are many fruitful opportunities for future work. Including explanations and fixing errors, AI algorithms like neural networks or others, such as probabilistic graphical models, are candidates to be used in these optimization problems with very large input dimensions for cross-layer and large-scale cybersecurity-related big data analytics. Currently, the computational load for the optimization algorithms used is significant. Thus, one of the promising follow-up steps of this study would be analyzing fast and scalable online optimization algorithms that can be computationally more efficient. Moreover, it would be promising to extend the current work for a cross-layer and/or inter-ERP DDoS cybersecurity event while including the quality of service and big data management issues in the optimization problems, which is an open research problem due to scarce research coverage. For this, close collaboration opportunities can be observed in utility theory, machine learning, and the design and analysis of algorithms fields. The ethics of artificial intelligence research, including cybersecurity, is an emerging issue. Thus, another possible future study direction could be an in-depth risk assessment for cybersecurity for big data-oriented ERP infrastructures, including the ethical aspects from the perspective of an artificial intelligence researcher in the scope of cross-layer and utility-theoretic-based cybersecurity and big data analytics. A collaborative discipline-specific conference, research project, or workshop can take place under various sponsorships to gather insights from the relevant domains in cross-disciplinary collaborations, further providing a platform for the formulation of proposals in these study dimensions. The workshop is also aimed at conceiving cyber hygiene and responsible AI outputs.

8. References

1. 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.
2. 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
3. Vaka, D. K. “Artificial intelligence enabled Demand Sensing: Enhancing Supply Chain Responsiveness.
4. Vankayalapati, R. K., & Syed, S. (2020). Green Cloud Computing: Strategies for Building Sustainable Data Center Ecosystems. Online Journal of Engineering Sciences, 1(1), 1229. Retrieved from https://www.scipublications.com/journal/index.php/ojes/article/view/1229
5. Eswar Prasad Galla.et.al. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions Educational Administration: Theory and Practice, 27(4), 1228 –1236 Doi: 10.53555/kuey.v27i4.7592
6. Syed, S., & Nampally, R. C. R. (2021). Empowering Users: The Role Of Ai In Enhancing Self-Service Bi For Data-Driven Decision Making. Educational Administration: Theory And Practice. Green Publication. Https://Doi. Org/10.53555/Kuey. V27i4, 8105.
7. Vaka, D. K. " Integrated Excellence: PM-EWM Integration Solution for S/4HANA 2020/2021.
8. Mohit Surender Reddy, Manikanth Sarisa, Siddharth Konkimalla, Sanjay Ramdas Bauskar, Hemanth Kumar Gollangi, Eswar Prasad Galla, Shravan Kumar Rajaram, 2021. "Predicting Tomorrow's Ailments: How AI/ML Is Transforming Disease Forecasting", ESP Journal of Engineering & Technology Advancements, 1(2): 188-200.
9. Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, Data-Driven Management: The Impact of Visualization Tools on Business Performance, International Journal of Management (IJM), 12(3), 2021, pp. 1290-1298. https://iaeme.com/Home/issue/IJM?Volume=12&Issue=3

10. Syed, S., & Nampally, R. C. R. (2020). Data Lineage Strategies–A Modernized View. Educational Administration: Theory And Practice. Green Publication. Https://Doi. Org/10.53555/Kuey. V26i4, 8104.
11. Vaka, D. K. (2020). Navigating Uncertainty: The Power of 'Just in Time SAP for Supply Chain Dynamics. Journal of Technological Innovations, 1(2).
12. Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Venkata Nagesh Boddapati, Manikanth Sarisa, An Analysis and Prediction of Health Insurance Costs Using Machine Learning-Based Regressor Techniques, International Journal of Computer Engineering and Technology (IJCET) 12(3), 2021, pp. 102-113. https://iaeme.com/Home/issue/IJCET?Volume=12&Issue=3
13. Syed, S. (2019). Roadmap For Enterprise Information Management: Strategies And Approaches In 2019. International Journal Of Engineering And Computer Science, 8(12), 24907-24917.
14. Venkata Nagesh Boddapati, Eswar Prasad Galla, Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Gagan Kumar Patra, Chandrababu Kuraku, Chandrakanth Rao Madhavaram, 2021. "Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times", ESP Journal of Engineering & Technology Advancements, 1(2): 134-146.
15. 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
16. 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
17. Mandala, V., & Surabhi, S. N. R. D. Intelligent Systems for Vehicle Reliability and Safety: Exploring AI in Predictive Failure Analysis.
18. 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