Review of Contemporary Philosophy
ISSN: 1841-5261, e-ISSN: 2471-089X
Vol 22 (1), 2023
Pp 6193 - 6209

Deep Learning-Enabled Big Data Analytics for Cybersecurity Threat Detection in ERP Ecosystems

[1] **Krishna Madhav Jha, [2]. Varun Bodepudi,[3]. Suneel Babu Boppana,[4]. Niharika Katnapally,[5]. Srinivasa Rao Maka,[6]. Manikanth Sakuru,**

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

Abstract

We propose to integrate deep learning and big data analytics to better manage cybersecurity threats that may emerge within an enterprise resource planning (ERP) ecosystem. Big data analytics on their own are insufficient for a rapidly growing threat landscape that becomes more sophisticated by the day. Deep learning can assist in analyzing complex patterns and structures in unstructured data. However, very few studies have hitherto combined these two technologies to specifically detect cybersecurity threats in an ERP environment. With this background, this analysis has two major objectives: (a) to investigate ways in which deep learning can be coupled with big data analytics to help contain cybersecurity threats in an ERP ecosystem and (b) to study the kinds of common threats, if any, that are currently present within an ERP environment.

This research is unique in that it presents an exclusive and comprehensive approach to detecting cybersecurity threats that may emerge within the internal processes and activities of an ERP ecosystem, using new and advanced analytical methods. In this study, cybersecurity threats were examined using various firewalls from different organizations located all across the globe, and the common related logs were collected. A new anomaly detection approach that integrates a deep learning technique into a big data analytics setup was initialized in order to check the new attempts and their patterns. The results have shown that the approach presented has the potential to be employed to detect fraud within ERP ecosystems, as well as gather insights into common cybersecurity threats that are generally observed. In other words, the detection of security threat factors is shown to be encouraging; thus, the practical research agenda has been proposed.

Keywords: Deep learning, big data analytics, cybersecurity, threat detection, cloud platform, fog platform, analytics, threat detection techniques, information systems, deep learning, trainable machine learning techniques, artificial intelligence techniques, advanced analytics approach, cybersecurity, enterprise resource planning, enterprise resource planning systems, intelligent security systems, advanced security operation centers.

Received: 16 october 2023 **Revised:** 29 November 2023 **Accepted:** 13 December 2023

1. Introduction

Business operations rely on efficient and uninterrupted performance of enterprise resource planning (ERP) systems and applications. For this reason, the significance of cybersecurity is increasing with the introduction

of cloud-based ERP solutions. In a hyperconnected world, these next-gen ERP systems are accessible by mobile applications, dashboards, and devices. Thus, ERPs are becoming favorite targets for hackers and cyber attackers. Since cyber threats have changing facets, cyber risk evaluation and mitigation through advanced detection techniques is an evolving area of research. The prime contract of this sophistication is tackling the multi-source and heterogeneous big data within the cyber-physical system of ERP.

Advanced analytics that includes artificial intelligence (AI) and machine learning (ML) have changed the dynamics of information and communication technology (ICT). It has improved efficacy and real-time availability within the outcomes of big data analytics (BDA). Specifically, ML has excelled in identifying hidden patterns within the historic or ex-ante data. However, evidence markedly showcases the incapability of traditional ML algorithms to learn complex interaction features. On the other side, deep learning (DL) offers advanced neural network architectures capable of learning associated, deeper feature interactions from historical data. In the literature, very few studies have employed the synergistic strength of AI-enabled deep learning for big data analytics for timely cyber threat detection within the traditional enterprise architecture ecosystem. Further, we foresee the future prospects of a sensor-rich cyber-physical system (CPS)-enabled augmented blueprint of the real world, which in the context of an organization represents a system with traditional IoT and cloud integrations.

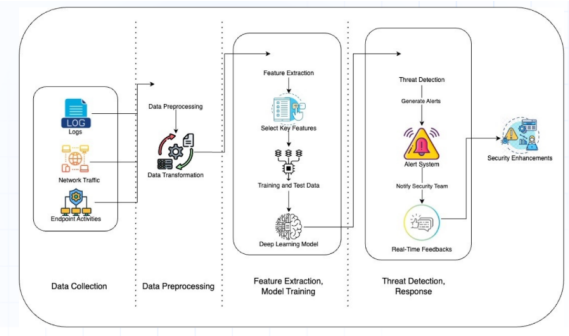

Fig 1: Deep Learning Architecture for Cybersecurity

1.1. Background and Motivation

Enterprise Resource Planning (ERP) has become an inherent part of global enterprises owing to their multifunctional nature. These systems observe transactions, which are essential to the success of modern business processes, making them prosperous targets for adversaries to launch different types of cyber threats. The number of exploitations on ERP systems was above 800 in 2021. The exploitations found in ERP ecosystems have different vulnerabilities, such as misconfiguration vulnerabilities, arbitrary file-reading vulnerabilities, and arbitrary code-execution vulnerabilities. These vulnerabilities can be used by adversaries to interrupt normal functioning, potentially causing severe financial and reputational problems. Exploitation of these vulnerabilities can result in the unauthorized disclosure of enterprise-sensitive data by network sniffing and the theft of enterprise-sensitive data, which often results in significant losses for organizations.

Historically, we frequently observe adversaries using attack vectors, considering phishing resulting from spoofed mail servers or unauthorized access to networking assets. Cobalt Strike is one popular commodity that adversaries have effectively utilized over the years to exploit vulnerabilities. The history of the incidents presented shows a clear inclination of targeting the web server application, indicating the importance of having servers that are locked down in a standard configuration. Deep learning has gained immense popularity due to applications that require functionalities like image pattern matching, pattern recognition, and detection in systems that are continuously producing big data. Most importantly, adversaries have already shifted their replies to known exploits with antivirus and firewalls with no observations from systems, which require more

sophisticated infrastructure for constant normal behavior tracking. The volume of security-relevant data and the range of patterns for meaningful analytics appears, therefore, as a big data problem.

1.2. Research Aim and Objectives

The prime aim of this paper is to explore a research gap related to the effectiveness of deep learning-enabled big data analytics in the area of cybersecurity, predominantly for the detection of cyber threats using big data. In tune with the research aim, the following are the research objectives: To identify and review various cyber threats that organizations are vulnerable to, especially in the case of ERP ecosystems. To evaluate the application of deep learning techniques in resolving cybersecurity issues that arise in the ERP ecosystems and present some of the methodologies already being adopted. To discuss some of the critical challenges in the contemporary world, particularly the question of security, and also suggest a theoretical underpinning, plus present a conceptual model to control the identified threats. Present a case for a real-world and proposed big data analytics architecture, finally pointing out some of the managerial implications that can be reaped from the work and giving a boundary conclusion. In line with the recent trends in business, coupled with the implementation of interconnected digital applications and cloud platforms, it is pertinent to discuss cybersecurity, which is currently a stand-alone subject in academic research and professional practice. Despite the importance of big data in an organization's ecosystem, very few scholarly reports exist on the operations of deep learning technology and especially big data for cybersecurity purposes, and more specifically in the case of the ERP. Identifying threats and designing measures for controlling them, in a way, will benefit both theoreticians and practitioners with a deeper understanding of the risks involved in adopting big data. In the context of big data, therefore, the main goal of this document is to provide an exploratory investigation into the developments and the importance of the aforementioned research questions. Given that an area of research has not received any insight, the paper takes a theoretical-cum-conceptual approach, illustrating the proposed model with the help of a real-world case architecture.

Equ 1: Big Data Integration and Parallelization

$$\theta = \theta - \eta \cdot \nabla_\theta \left(\frac{1}{|B|} \sum_{i \in B} L_{\text{model}}(X_i, y_i) \right)$$

where η is the learning rate, L_{model} is the loss function, and ∇_θ denotes the gradient with respect to model parameters θ.

2. ERP Ecosystems and Cybersecurity Threats

Enterprise resource planning (ERP) systems cover various business functions and provide diverse services ranging from managing and integrating important business operations and resources, such as customer relationship management (CRM), financials, human resources (HR), supply chain, production, and a plethora of others. Modern ERP systems are flexible, modular applications that provide a variety of functionalities to support business processes. ERP systems have a three-tier architecture, consisting of a database that contains the core business data, which is manipulated by a business operations tier consisting of middleware within the application server, which in turn communicates with the user presentation tier, providing a user interface via a web browser or other client. Access to ERP databases provides an array of intelligence and business data to conduct data analytics. At the same time, it is imperative to note that ERP systems are not immune to any type of security breach or unauthorized access, as these systems host a wealth of data useful to conduct fraudulent transactions or industrial espionage.

An ERP ecosystem is host to a variety of cyber threats, which include but are not limited to internal or external attackers, compromising the integrity of an ERP system by using zero-day vulnerabilities to cause a denial of service in existing systems to retrieve sensitive data, injecting ransomware campaigns, or even selling data on

shadowy online platforms. Data breaches and ransomware attacks are some of the most often observed attacks. The results of these attacks range from severe operational disruptions and hefty losses to brand erosion and litigation. The attack surface in the ERP systems could also range from injecting malicious code in the application layer, database, and underlying operating systems. The abuse of privilege roles in the ERP database to retrieve sensitive or confidential data, injecting malicious code in the database to retrieve sensitive data, and infecting hosts using ransomware to disrupt operations are some of the most recent observed attacks in the ERP ecosystems. Neither small organizations nor giant corporations in the world are left untouched by ransomware programmers. In total, the observed cost of these security breaches across industries is about $6 trillion annually. Small and medium-sized enterprises (SMEs) fall victim to nearly 60% of the security breaches. All these statistics make the ERP systems a lucrative business for anyone in the security market, as handling security threats is paramount in the ERP environments to maintain business functions.

Fig 2: ERP Ecosystems

2.1. Overview of ERP Systems

Enterprise resource planning (ERP) refers to the integrated management of core business processes facilitated by modern software and technology. The term "ERP" originally described a system designed to plan the use of enterprise-wide resources, i.e., to break down total business goals into production and operations plans. Most modern meanings reference software applications developed to record and manage enterprise data for activities undertaken by users in sales, manufacturing and inventory management, marketing, finance, distribution, accounting, human resources, and customer support—usually reporting on it in real-time. Alone in the field of supply chain management, ERP systems are covered by research, searching for analytical frameworks and their impact on business-to-business relationships. Fundamentally, an ERP system centralizes and integrates information and data across an organization, providing a coherent platform for diverse organizational operations and supporting the information management needs of different organizational functions. Using such an ERP system fosters the potential for creating operational efficiencies across entire organizational processes, often leading to a better-informed decision-making process. An "enterprise system" then represents a comprehensive industry term for an integrated software solution, enabling organizations to manage products, services, and actions, all the while tracking business transactions and providing timely, updated information on business trends for improved decision-making throughout the organization. ERP systems are typically based on broad modular software application packages, which could be designed to support processes covering multifunctional business areas such as human resource management, production activities, distribution management, sales management, accounting, finance, and others. This way, a single business-process function performs integrated roles, often simplifying data entry and data ordering, activities and communications across the entire enterprise. Modern ERP takes advantage of the latest developments in information technology, aiming to support new industries and markets. Organizations, faced with increasing global competition and interoperability requirements, often demand from these software applications significant adaptability to accommodate local requirements and support evolving company structures and practices.

2.2. Common Cybersecurity Threats in ERP Ecosystems

Today, the world is witnessing a growing number and complexity of cyber threats and risks with a specific focus on enterprise resource planning (ERP) ecosystems. The spectrum of cybersecurity threats is not limited to those listed above since cyber adversaries worldwide use a combination of old and new techniques to breach organizations and gain access to sensitive data. Some common cybersecurity threats that take advantage of ERP system vulnerabilities can be stated as follows:

1. Ransomware: Dishonest software-driven cyber attackers use ransomware to mix encryption methods with malware. Ransomware attackers demand a cryptocurrency payment; otherwise, they will not supply a digital key located on the server to unlock the encrypted data. Once ransomware penetrates the ERP system, cyber attackers encrypt all the confidential files and force the organization to pay the ransom; otherwise, the attackers destroy the data.

2. Phishing: Phishing is one of the most common social engineering techniques that cyber attackers use to compromise the ERP system by using email and fooling ERP users into thinking that they are genuine emails from a person. When ERP users click on a link in this type of fraudulent email, it installs unwanted software known as malware and ransomware that steals sensitive ERP business data.

3. Insider Threats: Insider threats compromise ERP security from within the organization. Insider threats are the most dangerous ERP threats and can be intentional or accidental. The insider threat is much harder to detect than the outsider threat because it is complicated and sensitive to determine why a trusted ERP user turns malicious, disgruntled, or phished to carry out a cyber attack on the organization. The integrity, confidentiality, and availability of the ERP system and information are crucial. Data loss can have considerably damaging effects on the business organization, including loss of customer trust and reputational harm, especially in cases where the stolen or exposed information is private. Additionally, the procedures carried out by the ERP organization can be interrupted by a cyber attack.

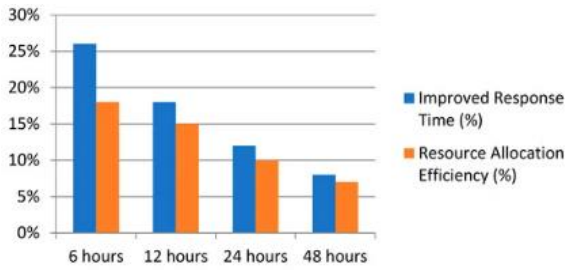

Fig : Graphical representation of adaptive decision-making results.

3. Big Data Analytics in Cybersecurity

The field of cybersecurity today is bustling with diverse kinds of attacks and evolves even as existing features are described. Cybersecurity is a primary research focus. Organizations presently possess a wealth of data that, if used properly, may help to recognize standard behavior in the ecosystem of ERP, as well as to diagnose violations in real time by means of some modern or traditional anomalous detection methods. Big data analytics are capable of developing methodologies to support the processes of planning, reaction, evaluation, and recovery via the development of new methods. Besides this, big data can not only be used to identify repeating patterns and trends, but also to identify repeated patterns and trends. Data-driven analytics for the vast amounts of data that should be collected in real time or near real time should become a core necessity for creating outlook and attitudes for proactive decision support. Besides diversified data, unstructured data, such as behavior monitoring data, can also be analyzed in a real-time manner regardless of origins.

All businesses in an organization go through cycles of development. At every stage of this cycle, security issues expand and are resolved during the process through dedicated technological efforts. They can no longer silo them into distributed pockets of standard and non-standard risk or threat detection; instead, they must develop the processes required. In this section, we assess the advantages and difficulties of conventional supply chain big data analytics, throw forward, and link it to ERP cybersecurity. While big data is a primary trigger in many firms for security strategy and action, some have lingered owing to a series of issues triggered through the implementation of big technology. The chief issue is the continued complexity of firms, and diverse silos of data can be found in southern development chains. For effective big data utilization, entire service localization and simplification must be brought about. Nevertheless, big data represents an unexplored chance for organizations to advance substantial developments to fittings, but also to software and tools to influence cybersecurity in the ERP ecosystem.

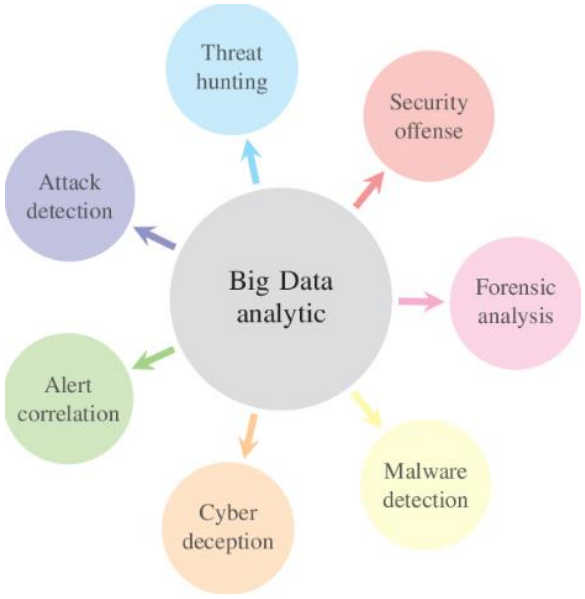

Fig 3: Big Data Analytics in Cybersecurity

3.1. Importance of Big Data Analytics in Cybersecurity

Every year, more digital assets are created, processed, and stored in cyberspace by individuals, organizations, and things in the forms of text documents, PDFs, images, speech, videos, logs, and so forth. With the advent of Industry 4.0, the Internet of Things, and the Industrial Internet of Things, data ingestion rates are expected to transcend yottabytes to zettabytes and go from zettabytes to brontobytes within the next few decades, assuming humidity, power, and material science resource constraints are overcome. Currently, the daily human data injections are approximately 2.5 quintillion bytes or 2.5 exabytes every day, and approximately 300 short message service messages are sent per second; approximately 60 billion emails are sent every day by world Internet users and world email users. This has created a host of follow-up products including unstructured, semi-structured, and structured data applicable in decision support systems and business intelligence for prediction, evidence-based, or prescriptive purposes across computing silos and scales, i.e., edge, fog, cloud, multi-cloud at unlimited or elastic scale, and hybrid multi-cloud architectures, systems, and services.

To this end, major advances have been reported in the literature leveraging big data analytics and its departure from big data technologies, thus enabling organizations to analyze petabyte or yottabyte size databases and data warehouses alike. Hence, these data-driven approaches support the detection of impersonation attacks and a wide range of cyber threats such as social engineering attacks, advanced persistent threats, crypto-currency mining attacks, ransomware attacks, rogue attacks, and insider threats that can be identified in near

real-time and even at future times with uncertainty in the prediction, through predictive and preemptive deep learning-enabled big data anti-attack mechanisms. Specifically, big data technologies and real-time big data analytics are used to detect anomalous behavior even though the attack features constructed are completely new and immune to any existing Intrusion Detection Systems and Intrusion Prevention Systems. Moreover, physical, cloud, edge, and 5G connectivity big data architectures are used for single or multi-tier, single or multi-domain ERP cybersecurity threat detections. For instance, based on the examination of susceptibility to attacks, big data analytics has detected up to 100 unknown threats, around 52 unknown attacks were accurately detected, and no false positives were produced, hence a 100% true positive rate was obtained.

3.2. Challenges and Opportunities

Big data analytics has transformed the cybersecurity threat detection mechanism of traditional ERPs from signature-based to anomaly detection techniques. While considering big data processing, cybersecurity professionals are likely to face several challenges given the volume, velocity, variety, and veracity of cybersecurity-relevant digital data. Companies are afraid of using big data analytics for threat detection as most of the threats come from their internal employees who have backend data access rights. Advancements in technologies, such as IoT, blockchain, and AI, have rendered ERP systems increasingly multifaceted. Inconsistent data, incorrect configuration files, and inappropriate handling by network administration and IT professionals may hurt the privacy of organizations.

The integration of big data analytics into cybersecurity can present both challenges and opportunities for organizations looking to make sense of this wealth of information. Organizations need to be able to tap into big data considering the speed at which information moves and the added volume to gain insights and a competitive advantage. However, the increasing complexity and size of the data set have also created an expanding skills gap. One of the major challenges for many data organizations is having the right talent in place to harness the potential of this data. The complexity and pervasiveness of these systems, combined with the large amount of potential security data they produce, can increase concerns. Apart from handling a high amount of data, protection is even more fundamental. In order to address these issues, a new set of compliance measures can be established to protect sensitive data and privacy. As organizations tackle these challenges, big data can be highly beneficial to business strategies. Executives, when making strategic or operational decisions, thus have access to the newest and most pertinent information. Security teams should likewise be able to react more quickly during an incident by increasing organizational resilience. Organizations might find it helpful to survey their employees on the use of innovative equipment and technologies and to recruit experts in doing so. Business security and education are thus strengthened, with a specific focus on big data. Some extremist shifts actually reveal just how young staff or security professionals recruit an attack by making these assaults. Working in tandem, organizations must partner with one another, therefore enforcing the importance of training staff and sharing concerns about data rights and privacy. Using advanced tools and systems to detect cyber threats, any business that drifts too far towards absolutely rejecting risk can significantly reduce its odds of being breached. By conducting a risk-benefit analysis on all innovative projects and new technology that comes into the company, cybersecurity professionals can walk the fine line between being protected and pushing the bar securely and vigorously.

Equ 2: Model Training and Loss Function

$$L_{class} = -\frac{1}{N}\sum_{i=1}^{N}\left(y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)\right)$$

where y_i is the true label (0 for normal, 1 for anomaly), and $\hat{y}_i$ is the predicted probability of the anomaly.

4. Deep Learning in Cybersecurity

Deep learning models consist of multiple hierarchically connected layers to learn from hierarchical features that could be anything like edges or corners in an image or word sequences in text data. To do this, the learning process affects the weights associated with these layers, and the end result after training can be an effective demonstrator on large-scale datasets. The primary advantage of using deep learning for cybersecurity is the capability of the model to rapidly process vast amounts of data. Hence, it can streamline threat intelligence in near real-time. Further, deeper networks can be efficient in pattern recognition, which is very relevant for the indicators of compromise and static malware approaches. In addition, these neural networks can operate in a continuous improvement loop that allows them to adapt to the evolving threat landscape. These systems can also self-improve and fine-tune their prediction ability.

Given the effectiveness of deep learning systems, these have been applied to various security problems, including malicious software detection. The deep learning systems employed for developing solutions for security have varying structures such as convolutional neural networks, recurrent neural networks, long short-term memory networks, shallow neural networks, autoencoders, and so forth. With different deep learning systems, they have been used in creating use cases, for example, C2 traffic and DNS tunnels in new detection with a different structure of deep learning, and even reinforcement learning is coupled into using it with a long short-term memory deep learning model for detecting ransomware. Obviously, the diversity of these systems and architectural innovation both show the scope of improvement and that multiple ideas about deep learning make it suitable for protecting organizations. The different uses show that the combination of deep learning systems can be united as a multimodal system to address multimodal threats that are consistently either IoT or SaaS oriented. Ongoing research in this space is at a significant premium cost for flexibility and customization. Despite the lack of data, there is a potential need to use deep learning in a security use case.

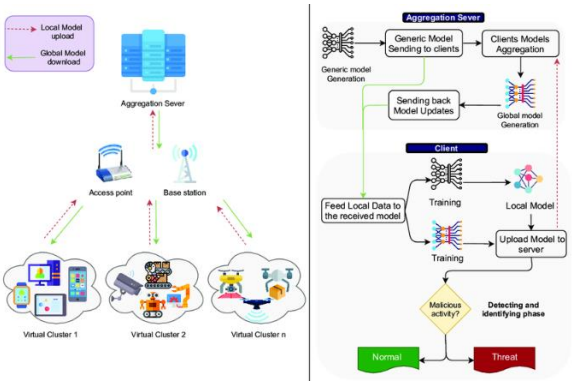

Fig 4: Federated Deep Learning for Cyber Security in the Internet of Things

4.1. Fundamentals of Deep Learning

• Deep learning provides a collection of techniques for learning representations of data. It comprises different architectures of artificial neural networks with increasing case learning representations. • Artificial Neural Network (ANN): Artificial neural network models are a set of algorithms patterned based on the functioning of human neural cells. Each neuron is a computational systematic unit. In a broader sense, an ANN model can predict output from inputs under consideration. • Supervised and Unsupervised Learning: In supervised learning, an algorithm learns from labeled training data and makes predictions. Unsupervised learning is a type of machine learning algorithm used to draw references from datasets consisting of input data without extensive knowledge of the output labels. • Feature extraction: It identifies and highlights significant features of the data in various forms. It is a process of dimensionality reduction by which an initial set of raw data is reduced to more manageable groups for processing. Architecture of Deep Learning: The architecture of deep learning consists of multiple layers of computing nodes that are generally divided into two phases, the layer of the input data and the output data layer, connected by computing layers known as hidden layers. • These hidden layers search for the best features of the input data to proceed with predicting the desired output. The feature-extracted hidden layers act on the parameters of the input layer for meaningful predictions. Importance of Data and Computation: Deep learning models are trained by learning from enormous amounts of data, making this an essential principle of deep learning. Furthermore, deep learning algorithms require significant computational resources in terms of time and hardware. Differences between Deep Learning and Traditional Machine Learning: Compared to traditional machine learning methods, deep learning techniques are more scalable and often yield higher accuracy. However, the model requires a good amount of data for training. Challenges: • Due to the increased complexity, learning models may overfit the training data. • Unlike traditional machine learning, deep learning models are harder to interpret. This can often lead to something like "black box" models because the features identified by each layer are not easily interpreted.

4.2. Applications of Deep Learning in Cybersecurity

Nowadays, there are various implementation areas for deep learning techniques in cybersecurity to enhance security measures. For instance, the possibilities in the cybersecurity context include, but are not limited to, malware detection, antimalware, antispam, network intrusion detection systems and host intrusion detection systems, anti fraud systems, anti-DDoS, multi-form solutions, firewalls, data loss prevention systems, application security, identity and access management, cloud security, endpoint security, mobile security, etc. Deep learning is proven to be an effective technique for these aforementioned applications to analyze data. In addition, it is discussed that the selection of the dataset, which is used for training deep learning models, is the most crucial issue to be able to produce efficient models. As an outcome, it is possible to decrease the likelihood of getting a false positive or negative result by having a good dataset structure when the training model performance is assessed. Moreover, deep learning algorithms are versatile in preventing a range of threats coming from diverse vectors according to the static signature-based traditional security mechanisms. Also, they can be a critical element in transforming preventative measures with both signature-based and emerging threat models. In particular, all preventive cybersecurity models have to be converted and supported by deep learning-based solutions that can offer advanced analytical models and save Cyber Operation Teams time during repetitive daily tasks. Hence, the success in operational efficiency increases greatly with deep learning solutions. In this section, there are some examples of deep learning in cybersecurity for different application areas. Some of the previous real-world examples of deep learning with cybersecurity applications may be summarized as follows:

• An automated system is developed with deep learning that combines neural networks and hierarchical clustering to detect varied threats from the network flow. • This previous concept develops a method that employs deep learning to detect malware by analyzing API calls. • A new study involves a combination of network intrusion detection systems and host intrusion detection systems from diverse vendors by leveraging deep representation and unsupervised learning to detect security anomalies.

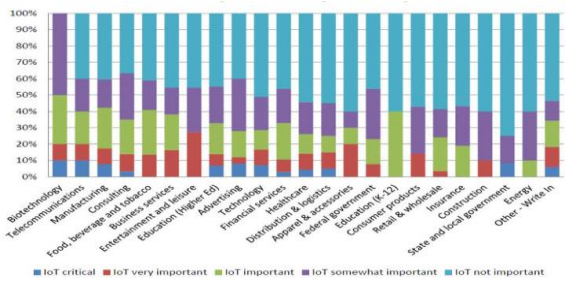

Fig : Big data - Benelux Intelligence Community - Results

5. Integration of Deep Learning and Big Data Analytics

Due to its predictive capabilities, deep learning is attracting attention along with big data analytics, which employ data with enormous volumes to make predictions based on existing knowledge. In the field of cybersecurity, when deep learning is integrated with big data analytics, it is possible to understand what will happen in the cyber environment using existing cyber human resource data. This is because, although it is difficult to share knowledge about each data point, it is possible to fully understand suspects with big data and human knowledge. As a result, using deep learning methods in big data analytics has the following benefits. By combining two datasets that have proven to be strongly correlated, it becomes possible to understand more, and it becomes possible to share knowledge whose validity has been confirmed. As a result, it is possible to respond quickly to the rapidly changing cyber environment, focus on enforcement, screening, and evidence to avoid false positives, leverage available data and human resources, and detect pseudo-attacks that mimic normal events and the early detection of attackers' preparation for a large-scale campaign attack using the findings of unacceptable conduct.

To level the concept of early indicators, site-specific information about assets, audit history, business processes, access rights, and user roles was collected and analyzed with big data, extracting deep learning insights. Deeper integration has emerged for both the evaluation of computational architectures and the scoring of sub-classifiers, as the first deep convolutional neural network used computer-aided processing to simulate data for cybersecurity and addressed the multi-domain attack on an e-commerce ecosystem. Deep learning and big data analytics commonly work on their own and operate independently. Additionally, big data works consistently on huge volumes of data, while deep learning and standard computer-augmented processing for cybersecurity act globally in a similar way. They are focused on new data or samples in the designated data system at first but have the potential to carry out domain transfer and hierarchical learning later. This means that big data screening and standard neural systems can act quicker in the individual stages and at the first level of broader computer-augmented processing. However, a deeper layer makes the system immature and more thorough, and a deep learning machine will be designed to refine and enhance the outcome. Successively, this establishes a mutual complementarity between deep learning and data processing, depending on the strong properties of each. Data analytics and deep learning are useful for understanding the root of unresolved security issues that can result in the use and exploitation of these and searching for potential early signs from vast volumes of existing information that can compel cyber hosts. However, some security cuts are difficult to find, particularly at the beginning. Although big data and deep learning analytics ultimately result in a comprehensive solution, further innovation is needed for wider results that have been actively involved in security. In the discussion below, the Cyber Situational Normality and Anomaly Detection Systems and Deep Learning Frameworks and the Mechanism for Simultaneously Combining them are discussed according to this context.

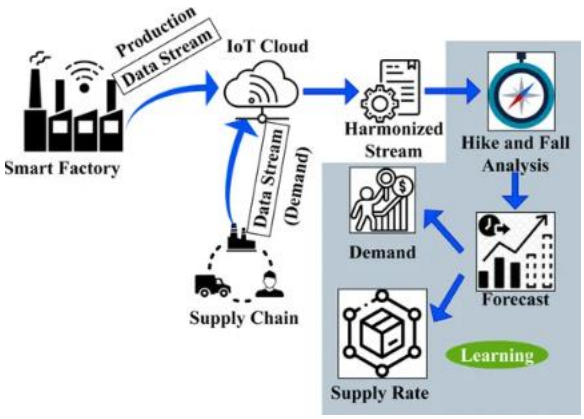

Fig 5: Integration of Deep Learning and Big Data Analytics

5.1. Benefits and Synergies

Our incentive to conduct cybersecurity threat analytics augmented with big data tools as an effective predictive maintenance strategy crosses paths with the aims of this preliminary investigation. There are even more advantages to synergizing deep learning and big data analytics for the detection of cybersecurity threats from a big data and ERP ecosystem security perspective. Deep learning's ability to process and analyze vast amounts of information quickly is well established. Cyberspace is no exception. This makes the job of sorting through huge amounts of data to examine them for any links that could reveal a security breach a more manageable task. Another benefit is that it can help you discover concealed relationships in either structured or unstructured data that security experts cannot see in their day-to-day tasks. For instance, in a cyber warfare study, big data analytics and deep learning technologies detected a suspected cyber attack being planned as an increase in certain traffic sharing economy-related topics. The incorporation of deep learning expands this predictive mechanism and can yield additional benefits. Security professionals can also be assisted by state-of-the-art deep learning algorithms in detecting and avoiding so-called zero-day threats, which are instances of new threats that have not occurred before. Big data analytics and deep learning can aid in the correct estimation or prediction of cybersecurity intruders to notify energy plant operators. By implementing real-time or close-to-real-time cybersecurity risk detection instruments in our study's ERP applications, we can take them to the next level. In order to maintain or enhance an organization's operational control, security response action automation can be incorporated. The aviation business has begun to implement deep learning and big data analytics in their analytical applications. The purpose of the analysis will be limited to enabling big data analytics augmented by deep learning for cybersecurity threat detection in ERP applications.

5.2. Technological Frameworks

A number of technology frameworks support the integration of deep learning with big data analytics in cybersecurity for enterprise resource planning (ERP) landscapes. Currently, cloud computing, distributed computing, and multi-parallel systems, collectively called big data frameworks, are used to store data and support its real-time analysis. Some important distributed computing systems provide useful architectures for engineering cybersecurity big data ecosystems. However, the mutual complementarity and superiority of these technological frameworks depend upon the specific business needs and capabilities of an organization. In the next section, a detailed discussion about the research directions and needs related to big data and deep learning for cybersecurity is presented.

Requirements for a Combined Big Data and Deep Learning System. Data pipelines and data processing frameworks are needed, including real-time analytics to capture instantaneously changing and large volume data streams. ETL processing includes A) sourcing ERP and cloud infrastructure logging data, transforming data, and loading it into the distributed file system and a minor portion into memory to reduce read time, and

B) memory processing to ingest data for the deep learning approach. Central knowledge base service tools are needed to pipeline data that supports a single system command service. Central email and inter-process communication tools are required to send messages to the cloud and business domain admin users regarding security threats. In addition, several communication-based tools are necessary to communicate with IT, business, labor, and firewalls. It is essential to collect and transform threat intelligence data into platform-based delivery mechanisms. Identification of the external component that supports the big data infrastructure is also necessary.

Equ 3: Anomaly Detection with Deep Learning Models

$$\text{Anomaly Score} = \begin{cases} 1 & \text{if } L_t > \delta \\ 0 & \text{if } L_t \leq \delta \end{cases}$$

where δ is a predefined threshold.

6. Case Studies and Practical Implementations

Several organizations currently use deep learning with big data analytics for cybersecurity threat detection in the ERP ecosystem. Since the cost of impending cyber threats is potentially disastrous, efficient ERPs are needed to handle important levels of network traffic with accurate real-time information. In this section, the essay presents case studies and examples highlighting the implementation of big data and deep learning in cyber threat detection in the domain of ERPs.

Case Study of a Global Market Leader in the Industry: A leading global market leader has been using big data and AI since 2019 to provide intelligent cybersecurity analysis that evaluates current security levels, generates behavior-based definitions, handles easy detection, and accelerates incident response processes. Detections are made using AI generative adversarial networks and autoencoders that get their data based on logs from a big data platform, focused on big data with artificial intelligence and machine learning. These advanced IT security solutions protect ERP systems by taking specific actions. Challenges – Cybercrime, fraud, breaking and entering, viruses and malware, breach exposed insider threat, cardholders and PII, internal sources and external hackers. Solutions – Algorithms, big data. Benefit – Artificial intelligence makes containment of hacking threats possible almost immediately. Fraud is also detected almost instantly. The ERP cybersecurity threat detection makes the organization a global market leader with a bug bounty and platinum membership. Lessons learned – The attack patterns are refined so that a more precise definition can be set of how cybersecurity systems should respond to attacks.

Restrictions of Case Study in Big Data: Missing historical data, commercial and open-source products and services used, hidden costs, hidden performance trends, BYOL fails, hidden performance, lock-in. The security world reduces danger by monitoring and analyzing information. This information includes events, logs, and data connected to systems controlling levels of infrastructure used to maintain warehouse cycles.

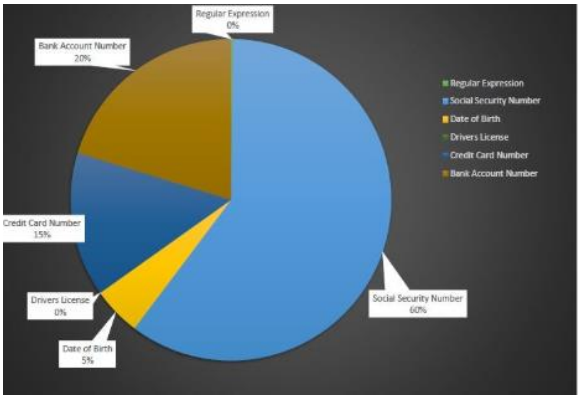

Fig : Sensitive Data Reporting and Visualization – Demonstrating Compliance

6.1. Real-World Examples

Real-world examples of big data analytics with deep learning in cybersecurity exist, and have been successfully implemented. Solutions have been presented in numerous sectors including: security information and event management for energy transmission networks, investigation of malicious insider threats in European linkages between historical infectious diseases, profiling and detection of intrusions in smart grids, anomalous behaviour detection in smart home IOT systems, and distributed scene-of-crime suspect mapping in urban environments. Traditional rule-based, signature, or white-list classification models are effective in certain domains but significant developments have occurred; for example, the first Convolutional Neural Network won the ImageNet Large Scale Visual Recognition Challenge. Notably, over 50% of security incidents involve an insider.

Specific to ERP systems, a recurring application is in anomalous behaviour detection and user authentication also known as adaptive machine learning. The application of recurrent CNN and Long Short-Term Memory networks for evaluating a user's transactional behavior has been considered. With respect to user authentication, a number of ERP vendors have also announced plans and progress around user behavioural analytics consisting of applying machine learning techniques to identify patterns from big data but specific applications of deep learning are limited. Insights from real-world applications of deep learning, traditional machine learning, and big data processing suggest a move towards supporting Advanced Persistent Threats in IT and, if previous history is any guide, provide further capabilities against OT systems. Importantly for an organization, which may not have the skills in house to implement state-of-the-art big data processing or deep learning themselves, the examples that follow demonstrate the successful transfer of academic research to a real-world problem either via an OEM or through acquisition.

A solution in healthcare on deep learning models for cyberbullying classification uses traditional machine learning methods as a baseline to compare the deep learning approach. An LSTM effectively improved performance at providing an organization the ability to detect, prevent and/or respond to cyberbullying. Globally there has been considerable research in the application of deep learning and reinforcement learning for spam detection across big data sets. The research has predominantly focused around email spam as part of outbreak detection predominantly. Two real-world examples where academic research has successfully been transferred to combat cyber-attacks with the focus on OT is in the explosion of business case solutions to support the detection of malware either via acquisition or as an original equipment manufacturer. In both instances the organizations are using deep learning, with a focus on network behavior.

6.2. Lessons Learned

After the completion of the risk analysis, the feedback from the workshops highlighted the main challenges, key recommendations, and next practices and trends. The analysis of the case studies and the feedback from the workshop collected a number of lessons learned and key takeaways. In terms of approaches, it is clear that organizations should align the technology and processes used with their organizational requirements. They suggest that business models should drive the need for technology, rather than the use of technology driving the business models. The testing of new technology in small projects was also a critical success factor in the implementations.

New initiatives can be complex to run and manage, and many organizations have failed to get deep learning and big data analytic initiatives off the ground and succeed. Much of this is due to a lack of understanding of the value that cyber analytics would deliver. Stakeholders, boards, and executives driving investment must take a more proactive position to ensure products and systems are secure. The running of cyber security as a cost center is something few boards can truly understand. The ease with which attackers can pivot from a compromised minor system to causing a true impact is not well understood. An intelligent view needs to be adopted. Security systems and practices are difficult to run and require continuous analysis and updates of security practices. There is a lack of trained specialists in both cyber analytics and the successful rollout of deep analytics. Staff at all levels of an organization need to be trained. Enough large-scale data feeds are required to drive good quality output from any security investment. When real data is limited, machine learning techniques can still be deployed; however, they may have effectiveness degradation. Finally, for all security measures and analysis, continual monitoring is required to detect new threats or adversary TTPs.

7. Conclusion

There are several key findings and insights emerging from the current essay. It is argued that deep learning, a subset of artificial intelligence, and big data analytics can be valuable enablers for cybersecurity within the ERP ecosystem of an organization. It is also claimed that today's organizations should invest in these advanced technologies to cope effectively with the increasing cyber threats targeting their valuable ERP systems and large volumes of sensitive enterprise data. We have outlined the benefits of the integration between sophisticated analytics and ERPs, such as improved threat detection capabilities, enhanced decision-making in near real-time, shortened incident response times, and improved operational efficiencies. We have also mentioned the ongoing challenges facing enterprises if they are interested in integrating advanced analytics into their current homegrown security products and proposed an architectural pattern. Organizational cybersecurity teams should be able to follow these guidelines and develop some non-traditional analytical-based scenarios to protect valuable enterprise data in the ERP ecosystem.

The proposed essay emphasizes the necessity of bringing new value propositions to organizations and encourages them to adopt continuous innovation paradigms. Given that data is considered the bedrock of modern ERPs, it is argued that organizations should have an opportunity to empower their current and future ERPs with big data analytics frameworks to increase their resilience to countless cyber threats. Hence, it forms a call to arms for all relevant academics, practitioners, and policymakers to take proactive actions regarding the enormous potential of big data in creating the organizational global competitive advantages of tomorrow. We have comprehensively addressed the urgent need for a certain technique in the analytics space to solve a specific problem in the organizational cybersecurity context. The current essay calls for organizations to start exploring the possibilities provided by deep analytics.

7.1. Future Trends

The next generation of deep learning and big data analytics is predicted to contribute significantly to the field of cybersecurity. In the coming years, these advancements could help to evolve the cybersecurity landscape and predict threats before they occur. Smart business professionals and scholars are focusing on improving AI,

emerging technologies, increasing processing power, and big data analytics. Consequently, we are now generating and utilizing big data for informed decision-making and to predict future trends. We expect that the data analytic part of big data will contribute more significantly in the future, allowing us to make data queries much faster. Indeed, data analytics tools are becoming faster and smarter in extracting data from big data, enabling computers and servers to analyze and predict the behavior of transactions.

We believe that artificial intelligence and machine learning models will significantly contribute to improving data science and the technology sector. These models identify common threats or unusual behavior and create alerts to resolve vulnerabilities. In our view, advanced detection, mitigation, and prevention measures can become part of a control framework focused on collective and cognitive intelligence concepts. As we predict verified threats using a deep learning approach, in the near future, AI and big data analytics will be able to adapt to user behavior using combined predictive and adaptive analytics to determine reasonable contributions and file sharing across users. As we know, sustained cutting-edge research can open new doors for the future, despite the fact that hackers are improving their skills. With the availability of big data, we aim to develop advanced security solutions by analyzing and maintaining large datasets and trend information for managing digital forensics. As technology such as AI, deep learning, and big data analytics improves, the business sector must adapt to a rapidly changing environment. We anticipate that publishers, academic researchers, and businesses will be altering their R&D strategies to manage potential digital threats in the future. Therefore, this section provides possible future directions in the years to come.

8. References

[1] Syed, S. Big Data Analytics In Heavy Vehicle Manufacturing: Advancing Planet 2050 Goals For A SustainableAutomotive Industry.

[2] Nampally, R. C. R. (2023). Moderlizing AI Applications In Ticketing And Reservation Systems: Revolutionizing Passenger Transport Services. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3280

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

[4] Vankayalapati, R. K., Sondinti, L. R., Kalisetty, S., & Valiki, S. (2023). Unifying Edge and Cloud Computing: A Framework for Distributed AI and Real-Time Processing. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i9s(2).3348

[5] Eswar Prasad G, Hemanth Kumar G, Venkata Nagesh B, Manikanth S, Kiran P, et al. (2023) Enhancing Performance of Financial Fraud Detection Through Machine Learning Model. J Contemp Edu Theo Artificial Intel: JCETAI-101.

[6] Syed, S. (2023). Zero Carbon Manufacturing in the Automotive Industry: Integrating Predictive Analytics to Achieve Sustainable Production.

[7] Nampally, R. C. R. (2022). Neural Networks for Enhancing Rail Safety and Security: Real-Time Monitoring and Incident Prediction. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 49–63). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2022.1155

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

[9] Sondinti, L. R. K., Kalisetty, S., Polineni, T. N. S., & abhireddy, N. (2023). Towards Quantum-Enhanced Cloud Platforms: Bridging Classical and Quantum Computing for Future Workloads. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3347

[10] Siddharth K, Gagan Kumar P, Chandrababu K, Janardhana Rao S, Sanjay Ramdas B, et al. (2023) A Comparative Analysis of Network Intrusion Detection Using Different Machine Learning Techniques. J Contemp Edu Theo Artificial Intel: JCETAI-102.

[11] Syed, S. (2023). Shaping The Future Of Large-Scale Vehicle Manufacturing: Planet 2050 Initiatives And The Role Of Predictive Analytics. Nanotechnology Perceptions, 19(3), 103-116.

[12] Nampally, R. C. R. (2022). Machine Learning Applications in Fleet Electrification: Optimizing Vehicle Maintenance and Energy Consumption. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.8258

[13] Vaka, D. K. " Integrated Excellence: PM-EWM Integration Solution for S/4HANA 2020/2021.

[14] Kalisetty, S., Pandugula, C., & Mallesham, G. (2023). Leveraging Artificial Intelligence to Enhance Supply Chain Resilience: A Study of Predictive Analytics and Risk Mitigation Strategies. Journal of Artificial Intelligence and Big Data, 3(1), 29–45. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1202

[15] Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, et al. (2023) An Evaluation of Medical Image Analysis Using Image Segmentation and Deep Learning Techniques. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-407.DOI: doi.org/10.47363/JAICC/2023(2)388

[16] Syed, S. Advanced Manufacturing Analytics: Optimizing Engine Performance through Real-Time Data and Predictive Maintenance.

[17] RamaChandra Rao Nampally. (2022). Deep Learning-Based Predictive Models For Rail Signaling And Control Systems: Improving Operational Efficiency And Safety. Migration Letters, 19(6), 1065–1077. Retrieved from https://migrationletters.com/index.php/ml/article/view/11335

[18] Mandala, G., Danda, R. R., Nishanth, A., Yasmeen, Z., & Maguluri, K. K. AI AND ML IN HEALTHCARE: REDEFINING DIAGNOSTICS, TREATMENT, AND PERSONALIZED MEDICINE.

[19] Polineni, T. N. S., abhireddy, N., & Yasmeen, Z. (2023). AI-Powered Predictive Systems for Managing Epidemic Spread in High-Density Populations. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3374

[20] Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Venkata Nagesh Boddapati, Manikanth Sarisa, et al. (2023) Sentiment Analysis of Customer Product Review Based on Machine Learning Techniques in E-Commerce. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-408.DOI: doi.org/10.47363/JAICC/2023(2)38

[21] Syed, S. (2022). Breaking Barriers: Leveraging Natural Language Processing In Self-Service Bi For Non-Technical Users. Available at SSRN 5032632.

[22] 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

[23] Syed, S., & Nampally, R. C. R. (2021). Empowering Users: The Role Of AI In Enhancing Self-Service BI For Data-Driven Decision Making. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v27i4.8105

[24] Nagesh Boddapati, V. (2023). AI-Powered Insights: Leveraging Machine Learning And Big Data For Advanced Genomic Research In Healthcare. In Educational Administration: Theory and Practice (pp. 2849–2857). Green Publication. https://doi.org/10.53555/kuey.v29i4.7531

[25] Mandala, V. (2022). Revolutionizing Asynchronous Shipments: Integrating AI Predictive Analytics in Automotive Supply Chains. Journal ID, 9339, 1263.

[26] Korada, L. International Journal of Communication Networks and Information Security.

[27] Lekkala, S., Avula, R., & Gurijala, P. (2022). Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity. Journal of Artificial Intelligence and Big Data, 2(1), 32–48. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1125

[28] Subhash Polineni, T. N., Pandugula, C., & Azith Teja Ganti, V. K. (2022). AI-Driven Automation in Monitoring Post-Operative Complications Across Health Systems. Global Journal of Medical Case Reports, 2(1), 1225. Retrieved from https://www.scipublications.com/journal/index.php/gjmcr/article/view/1225

[29] Seshagirirao Lekkala. (2021). Ensuring Data Compliance: The role of AI and ML in securing Enterprise Networks. Educational Administration: Theory and Practice, 27(4), 1272–1279. https://doi.org/10.53555/kuey.v27i4.8102