Journal of Artificial Intelligence and Big Data Disciplines (JAIBDD)

International | Peer Reviewed | Open Access | Online

A Comprehensive Study of Big Data Utilization in AI-Driven ERP Cybersecurity Applications

Gowthamm Mandala
Biological Health Sciences
Purude University,
West Lafayette, USA

Abstract : The term "Big Data" refers to data that has massive volume, is varied in nature, and is generated at a high velocity. This data is difficult to process using conventional database management tools, and it grows over time. Cybersecurity is not limited to securing software applications or infrastructures; instead, it focuses on safeguarding data systems from any kind of breach or unauthorized access. Enterprise Resource Planning, or ERP system, is an information system that integrates all business transactions, and the data present in the system flow between various units or departments of the company. Such systems are more often targets of cyberattacks because of the data they hold. AI-driven ERP cybersecurity applications are imperative for securing such systems against modern cyber threats. AI technologies provide automation, and when integrated with Big Data, it becomes a stronger tool for enhancing the security of any data system.

This study is focused on AI and Big Data techniques that can be used in ERP cybersecurity systems. The proposed methodology can be used by any cybersecurity developer for building a data processing system or AI mechanism that can effectively process data from an enterprise system or any data system. Associative classification techniques can be impressively effective compared to conventional classification solutions in the development of an AI algorithm for detecting cyber threats against ERP systems. It is more effective in comparison to traditional algorithms, as very few works are available on associating associative

rules on a complete log file of an organization containing organizational data for work purposes. Additionally, the proposed framework can be imperatively helpful for real-time surveillance and data management systems and may lead to future growth in the cybersecurity and digitization domain.

Keywords: Big Data, Artificial Intelligence, Enterprise Resource Planning, Cyber Security, Internet of Things, Application Security, Worldwide Interoperability for Microwave, Wireless Body Area Network.

1. Introduction

The increasing digitalization of enterprise management systems, particularly ERP, has posed a number of demanding challenges for today's cybersecurity environment. With some studies reporting violations by cyber-attacks on these systems every 39 seconds, the absence of automated security strategies is evidence of why safety has failed to keep up with technological advances in AI analytics and automated Big Data systems. A lack of integration between AI and Big Data development efforts contributes to the continued limitations of the current systems. Emerging results from the recent literature have elevated AI and Big Data technologies as significant instruments for enhancing the situational awareness-oriented reactive, preventive, detective, and anticipative dimensions in the evolving cybersecurity sector. The blending of AI and Big Data is generally thought to maximize the capacity of security-relevant data to produce evidence-based safety services. This is particularly significant in recent studies of ERPs that have started to incorporate these new information systems with AI and Big Data.

Successfully advancing cybersecurity in the ever-growing world of AI-driven ERPs requires a comprehensive analysis of Big Data applications. This involves not only a definition and instance of Big Data technologies, AI with case indications for the period 2008–2019, and a collection of MIQs on the current research scenario in AI and Big Data in combination with cybersecurity in general, including public, AI-related, and ERP cybersecurity issues. The images are helpful for those additional researchers who may be interested in this area. In addition, the picture denotes the need to assess and integrate AI and Big Data understanding in the contemporary cybersecurity landscape, largely in current ERP studies and research focuses. The snippets aren't about addressing public, defense, or cybersecurity issues. Rather, the rest of the investigations on Big Data technologies were seldom found. An attempt was also made here in our first published conceptual article to define Big Data technologies in general. This research is an effort to address questions such as "What is Big Data and what problems is it designed to fix?", "What is Big Data's founding concept?", "What is the average size of Big Data collections?" or even "How often does Big Data change?" This article is aimed at an AI-related and cybersecurity-related expert in Big Data technologies. The structure of this article is described below at a glance. A questionnaire lays out the errors ahead of time and its goals prior to initializing the study. It is also useful for better documentation of the MIQs' future implementation process, providing a clearer context. Finally, the picture reflects the progress they have made in recent years, proving they are

new and important. It identifies future research lines constituted by the MIQs and Big Data technology classifications, eventually reflecting what AI and Big Data have accomplished in recent years.

Fig 1: AI In Cybersecurity

1.1. Background and Significance

In recent years, an enormous volume of structured and unstructured data has emerged due to the exponential increase in data generation in real-time. Analyzing big data can reveal useful information and knowledge for enhanced security measures in enterprise resource planning (ERP) systems. The utilization of big data includes the detection and elimination of known and zero-day threats, rapid incident detection and response, log file analysis, insight into new patterns of cybersecurity threats, and policy non-compliances. Historical data analysis identifies unusual patterns of data movement within and beyond the application. Big data, in combination with artificial intelligence (AI), increases the scope and capacity for the analysis of various types of user activities and understanding the impacting repercussions of malicious activities on company reputation.

Currently, the size of digital data production is increasing at an unprecedented rate, reaching 44 zettabytes by 2020. Every minute, there are 404,999 installs and downloads, 500 hours of new videos on YouTube, 18,100,000 texts, 104,000 calls, 3,700,000 searches on Google, and 188,056,000 sent emails. Owing to the substantial upsurge in data generation, sophisticated enterprise resource planning (ERP) systems with multifunctional modules and extreme features have been developed to support organizational processes, with demand surging due to their reliability, usability, and storage capacity. Among these modules, the customer relationship management system is popular, with its enormous storage capacity to store customer details and statistics, and human resource management applications. In general, the volume and number of threats and observed exploit techniques have increased over time. The newer published malware can bypass all types of antivirus; there is a significant increase in polymorphism and metamorphism of Windows executables. The present antivirus can detect a maximum of 70% of the total threats, which is where network security becomes crucial to catch the zero days. In practice, security professionals reverse-engineer dominant threats and generate a created signature to catch future threats. Organizations do not have full-time security professionals; these threats exploit vulnerabilities, leading to fundamental problems. These are some of the current issues that we are facing with sensitive data stored in companies. Scalable learning designs in AI and algorithms, such as artificial neural networks, based on AI can predict upcoming cyberattacks.

1.2. Research Objectives

The objectives of this comprehensive study encompass a clear and concise explanation of the research study itself. The study's objectives are to present Big Data and AI's integrated role within the cybersecurity aspects of ERP. Utilizing the given purpose, research questions, and scope of the study, the intention behind developing a brief understanding of the background around ERP and AI implementation rather than delivering a detailed analysis within the paper is based.

The main purpose associated with the objectives is to derive effective working methodologies towards data management, AI-driven processing with data integration, algorithms, and performing analysis over the management outputs for identifying threats. Secondly, a study has been directed to identify and consult adequate solutions by adopting contemporary research and industry recommendations, tackling the operational issues associated with cybersecurity. This study also discusses which aspects in the cybersecurity paradigm of AI and Big Data can be studied, analyzed, simulated, or synthesized. This study would also look at researching future aspects of AI and Big Data in cybersecurity. The study will also contribute to supporting future researchers, sectors, professionals, and industry advisors. Lastly, there would also be industry contributions presenting a comprehensive comparative analysis of existing industry implementation and proposed AI-Big Data approaches which could produce the future course of action.

The research objective is to investigate how Big Data and AI can be integrated into the cybersecurity aspect of the ERP networking system. More specifically, the given research study is based on the artificial intelligence system, its database, and algorithm considering increased usage and its limitations across ERP networking systems' performance. However, the aim is to conduct a study surrounding AI for intrusion detection in ERPs, how it is used from a technological standpoint, advantages, and future analysis. The focus is on AI-ERP systems. The present study is associated with AI-ERP systems in order to show the role of Big Data and to identify needed research. The review paper goes in a systematic direction, addressing the given objective, in order to provide a depth of insights from the paper. The study highlights two index databases to manifest the works for ERP targeting AI or AI for the intrusions.

1.3. Scope and Limitations

A comprehensive study of big data, AI, and ERP systems is not possible within the scope of this paper, nor is it the focus. Instead, this paper provides a complementary review with three main objectives. Firstly, it reviews existing literature in the context of relevant studies from different domains. Secondly, it reviews real-world big data utilization processes in the context of AI-assisted, ERP-enabled cybersecurity applications. This is the main research objective and general context of this paper. The final research objective is to extend the existing view of cybersecurity in ERP systems, focusing on AI, big data, and hybrid solutions.

The paper describes the various cybersecurity aspects of big data at the intersection of AI and ERP in the application layer. Our study investigates and overviews specific and manageable big data material to provide new and unconventional AI-assisted, ERP-supported, and big data hybridization viewpoints and applications in the context of cybersecurity. In the current scientific domain, no deep learning techniques-based cybersecurity approaches have been done with this holistic big data viewpoint. However, this research has some limitations. The non-availability of application-based, provable datasets for AI based on the newness of the proposed viewpoints and findings is a major limitation of this research.

If datasets were available, it would be very helpful. This research does not provide any statistical or experimental analysis; rather, it suggests solely AI-ERP integration based on AI findings and cybersecurity challenges that could be worked on. Additionally, because of ethical biases and hacking complications, system developers and administrators are not disseminating or sharing their attack datasets. Consequently, this research provides a high-level overview of global cybersecurity aspects in the AI-ERP intersection.

Equation 1: Data Preprocessing in Big Data (Data Quality and Transformation)

$$x' = \frac{x - \mu}{\sigma}$$

Where:

- x = original data value,
- μ = mean of the dataset,
- σ = standard deviation of the dataset,
- x' = normalized value.

2. Foundations of Big Data in AI-Driven ERP Cybersecurity

The concept of big data can be thought of as those large volumes of data that cannot be managed effectively by traditional relational database management systems. The analysis of big data includes systems and applications that are able to process very large datasets that traditional systems cannot process well. The volume of big data emphasizes its massive, interactive, and dynamic nature, which includes scalar data, and the portion of scalar data is constantly increasing with time. Big data has many properties including volume, variety, and velocity. Big data introduces a real tsunami of information. In addition to the above three primary characteristics, big data has a fourth characteristic known as veracity, as it refers to the quality and trustworthiness of data. The fifth characteristic, which is a rapid growth by some researchers, is named as the fifth V, namely value; the information hidden behind the potential also has the value of being exploited.

The integration of artificial intelligence with cybersecurity deploys a proactive solution. As AI has revolutionized almost every business and industry, it is also gaining importance in the context of security applications specifically for detecting unknown attacks, insider threats, making a security policy, monitoring, and alerting. Although the exact amount of AI incorporated with cybersecurity costs heavily for implementation, its cost is truly significant and holds a significant place in the security system of an organization. AI technologies like data correlation, machine learning, and data classification are helpful in fraud detection. AI enables faster identification of new threats and real-time threat protection, giving an improved user experience. The most commonly used three AI techniques provide a basis for the development of anomaly-based IDSs, which are machine learning techniques, data mining, and data analytics techniques using visual analytics, etc. In developing this, they deploy the combination of these techniques to carry out their tasks. Unlike these two previous AI techniques, machine learning and data mining only extract relevant data from the network, analyze it against predefined attack patterns, and then create useful information based on the scores and the patterns. Enterprise resource planning systems are interdependent on each module and specially designed to meet ongoing organizational needs that are expanding in growth. Moreover, by adding new modules and functionalities as an increase in demand, the number of developed odd data increases. ERP systems mainly work on their own customized hardware and data stored in a central database to enable decision-makers to make quick decisions using real-time data. Given their outstanding features, the use and development of ERP systems is exponential, and their data must be kept secure. In order to avoid any in-house security attack, the enterprise security administrator should monitor all these activities. To clarify the importance of big data, AI, and ERP cybersecurity, we introduce our studies as the combination of key challenges leading to the formulation of a robust and effective AI-driven ERP security analytics data framework. In the next section, we introduce the methodologies that are relevant to our study, which therefore provides a cyber-attack ontology.

Fig 2: Big Data in AI-Driven ERP Cybersecurity

2.1. Overview of Big Data

The term "Big Data" describes datasets that grow so large that they become difficult to capture, store, manage, and analyze. There are three main characteristics a dataset must present in order to be considered as Big Data: volume, variety, and velocity. Big Data processing can be useful in many contexts, although processing becomes more complex as data heterogeneity increases, due to its structure or its generation speed.

For instance, Big Data analytics can be used to improve cybersecurity. The basic idea is to take the huge amount of data that networks and endpoints generate daily, process it in close to real time, and help answer the fundamental security questions of "What is happening on my network?", "What should be done?" and "How to do it?" This addresses the challenge of modern-day security, because it is characterized by the daily interaction between data generation and data analysis. This everyday larger amount of connections and network attacks needs a real-time response, so threats can be assessed and the system reconfigured as part of the recuperation strategy.

There are many types of data that are crucial to cybersecurity: - Structured logs such as databases and web server logs. - Unstructured data such as security reports and documents. - Email, mobile, and web interactions and other network traffic. - Outputs from various collections of intrusion

detection systems, firewalls, and behavioral anomaly tools. Big Data can be useful in many contexts, including cybersecurity. However, in this domain, processing becomes more complex as data heterogeneity increases, due to its structure or its speed, i.e., the real-time processing. Managing petabytes of data in log files originating from various sources is therefore a significant challenge.

2.2. AI Techniques in Cybersecurity

In recent times, various artificial intelligence (AI) techniques have evolved and have crucially fortified cybersecurity. They facilitate an early identification of emerging threats and improve the finely grained analysis of diverse attack strategies and associated risk factors. Machine learning, deep learning, as well as natural language processing (NLP) paradigms are designed to enhance the detection of attacks, online fraud, and privacy violations against advanced persistent threats (APTs) and related post-exploitation tactics, such as data theft, customization of executables, stealth, moving laterally, and establishing persistence. Since AI is capable of recognizing patterns and behaviors that escape human observation and analyses, it is an asset in the quest for enhanced security. AI has a critical impact on real-time decision-making in combating cyber threats, and a recent study on this complex interdisciplinary field of AI and IoT forensics offers deep insight. The study reinforced the fact that AI mechanisms aid in efficiently detecting security intrusions and emerged as a significant tool in securing and protecting IoT and edge devices and platforms. Moreover, AI's strength in analyzing underlying historical data enriched with semantic and statistical inferences has had a great influence and brought about human-machine convergence, indicating that the domain is maturing significantly. AI algorithms can be applied to IoT/IIoT and cloud cybersecurity, specifically to the protection of critical enterprise information system resources such as enterprise resource planning (ERP) and not only limited to the detection aspect. In fact, there are cybersecurity products from leading companies that follow a similar approach, especially for the secure access services edge (SASE) architecture. The power of AI algorithms is harnessed to continuously monitor and secure on-premises systems such as HR, supply chain, and manufacturing using AI technology. In addition, AI is being combined with quantum-safe cryptography to secure blockchain applications and networks in post-quantum cryptography, biological-based defenses against cyber-physical system threats, and adaptive machine learning to secure the IoT on software-defined networking. The AI models, when adapted to and constantly reviewed against the generic ERPs and organizations' data, correlate discrepancies and security violations against standard policies, preventing, for instance, the reset marathon and suspicious acts. AI offers game-changing new possibilities in cybersecurity and forensics, but it also poses major potential difficulties. It needs to be seen in this context.

2.3. ERP Systems and Security

ERP systems pose unique security challenges in both the operational environment and the vulnerabilities these systems present. Until the end of 2018, a pitiful 64% of CIOs could say that their current or intended ERP system was secured. In 2018, the practice of maintaining large software systems was still based on methods and ideas of the late 1960s. In today's interconnected world, an ERP system is essential for most businesses. It has become the most complex and integrated software package available to business.

ERP systems are becoming critical to the operation of businesses. Therefore, organizations have been investing significant efforts in enhancing the security of ERP systems. Social engineering exploits human interaction to change the values of critical data. Perhaps even more powerful is the effect of such information on the inherent and enduring battles between 'what business wants' and 'what the organization can do'. Awareness and ongoing training of all users in the form of an ERP policy is advocated. The following control measures are suggested: transmit many protected data elements with encryption. Both ERP systems can utilize big data in a number of different ways. To investigate what data is ongoing in real-time, one technique would be to monitor passively the traffic to and from the database. A prototype solution uses big data and machine intelligence to check if artificial data attempts used to prevent risks are indeed working. There are numerous researchers that drive forward big data and ERP security. Such work would generate information to prevent risks and threats to the ERP application systems. From monitoring hazardous error data from an ERP system to tracking the audit and fraud data for buyers, researchers are exploring data information that would help security experts to secure the ERP. Such information would be useful in answering complex and important research questions such as: what do industry CISOs need for ensuring ERP security success; what ought not to bother them? How best to transform the ERP to take full advantage of big data intelligence? While it is a step forward in ERP security understanding that is required to adequately understand the business risks of ERP security, there needs to be a fundamental understanding of how far ERP security weaknesses can lead to an increase in enterprise risk. Trend analysis and lessons learned from studies of attacks and cyber breaches have identified: the majority of information attacks into many businesses first take place between the hours of 7:00 PM and 12:00 AM when network and business site activity reaches its minimum. These overnight attackers principally target certain enterprise data repositories using neatly packaged, modified, and infected ERP business system settings. Given ERP systems form the location of the systems of reality that a significant proportion of IT business activity is stored in, forecasters are predicting not if but when a major cyber-attack will be launched into an unprepared business by using chief risk officer tools. Results of the first 21 years of chief risk officer thinking have indicated that an astonishing two-thirds of management decisions are based on intuition, not facts or ERP systems. Business has been prepared for the normal and is managing in the down phase of the frequency of the snowflakes and three invisible asset bubbles. Cyber breaks will enter the asset bubble of recognition. Cyber will deliver major events with significant financial risk that will threaten the survival of the enterprise to be reached using risky change and all of business's five deadly types of risk regularly on this list, not just information risk, including the cyber threats to the business from within.

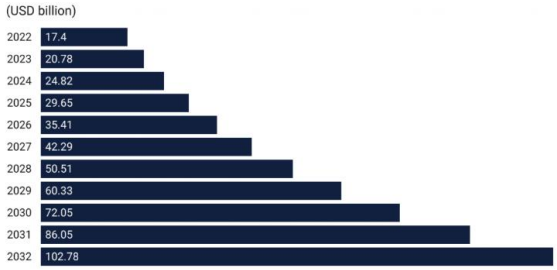

Fig : AI in Cybersecurity Statistics and Facts

3. Integration of Big Data and AI in ERP Cybersecurity

Modern businesses rely on advanced levels of data processing efficiency and knowledge discovery and intelligence to realize organizational security and protection from harmful software, unsanctioned access, and data breaches. A tremendous rise in the amount of data storage, access, and firm-based data collection and processing necessitates careful consideration for managing these large data stores both safely and effectively.

For businesses and organizations adopting such solutions, the large amount of data constitutes a gold mine of information, a vast source of business intelligence that enables them to make informed decisions regarding security strategies and infrastructures. In comparison to smaller datasets, as the size of the data stored by firms increases, the foundation of data-driven improvements in cybersecurity is heavily based upon large data and particularly upon the processes that can be used to collect, process, and make valid interpretations from potentially high-volume, high-velocity, and high-variety enterprise resources. Interactions between large data and intelligent technologies and their application in advance with intelligent technologies in data mining disruptive technology necessitate consideration of the rapidly evolving field of cybersecurity wherein both human users and automated systems might have to operate with incomplete, imprecise, and uncertain patterns of attack.

While understanding the potential benefits associated with the integration of large data and intelligent technologies, there are systematic advancements and granular methodologies to study such developments in order to gauge their impact on the evolution of intelligent technologies within cybersecurity research and practice. Large data can be utilized to assist and model cybersecurity processes and predictions of cybercrime, to detect and respond to developing threats, vulnerabilities, and actors. From a cybersecurity perspective, large data analytics can be employed in several ways. For instance, such techniques can rely on data compiled from firm-internal security event sources to establish a baseline of regular or 'normal' system behavior. Large data can be analyzed using intelligent technologies and tools to detect anomalies in the data that can provide insight into potential security-related threats, trends, and innovative attack surfaces that decision-support systems can utilize in 'learning-based' predictive alerting systems. Intelligent cybersecurity systems are capable of utilizing large data techniques coupled with intelligent technologies to significantly filter, collect, process, and analyze large volumes of data from a variety of enterprise data sources that previously would require manual processes. In this sense, intelligent systems can be utilized as an assistive tool to actively monitor a large quantity of cybersecurity-related inputs and act as an autonomous system to take further action, avoiding the increasing risk associated with slow decision-making speeds. Intelligent systems can be trained to become increasingly effective in handling a wide array of potential risks and hypotheses utilizing massive amounts of cybersecurity data.

Fig 3: Integration of Big Data and AI in ERP Cybersecurity

3.1. Data Collection and Processing

In a well-rounded cybersecurity program or security operations center (SOC), collecting sample data is crucial regardless of the security tool; such data can lead to actionable conclusions. A variety of structured and unstructured information is collected from various sources: antivirus, firewall, and data loss prevention devices; operating systems; databases; networks; and applications, to name a few. This operational data is formally called logs. The plethora of log data needs preprocessing, which involves cleaning, transforming, and analyzing these datasets for Extract, Transform, and Load into systems that store massive amounts of data for diverse analyses. Not all of the incoming data is valid, of top quality, and relevant.

IT-related log information, for example, includes pieces of data that are transitory, in that the information is outdated after a certain period of time. The property of removing outdated data from the analytic data is one way in which the "value" of big data AI security operations can be obscured and artificially depreciated. In principle, the linkage between the maturity of a cybersecurity infrastructure, the regulations under which it is operating, and the requirements for big data analysis is especially clear. Unlike the academic "need for data purity," compliance with crime-fighting, consumer, or global regulation mandates specific minimum data storage policies related to operational tracking and retention periods. Furthermore, compliance-related processing places enormous pressures on corporate security organizations because of the amount of time and data records required to deal with an individual potential data breach incident or incident investigation. Calls to reduce data storage or apply privacy laws reduce the utility of large dataset AI security systems from a purely operational perspective. Countering the mantra of big data is the prevailing wisdom about the certain huge quantity of events in the security world.

3.2. Anomaly Detection and Threat Intelligence

Anomaly detection has a pivotal position in the cybersecurity paradigm. It is the process of recognizing differences in data patterns that do not comply with normal actions. Hence, it can be used to identify security risks. Advanced AI-driven learning procedures can be used to achieve a high level of anomaly detection. For this, it is necessary to obtain a clear understanding of the normal system actions and to establish a baseline for the system's habits to match with any irregular incidents. Threat intelligence is the utilization of obtained evidence on planned attacks, exploitation, threat behaviors, or signs of threat to foresee possible future threats.

Threat intelligence provides cybersecurity and physical effectiveness with the signs to help correspond to a situation using the enrichment method. Enrichment enables security enforcers to improve threat indicators by linking them to known examples of risk-related data. Threat intelligence sources vary widely, including sensory data collection systems, information sharing partnerships, commercial threat feeds, open-source information, attacker risk assessments, organization data collection processes, and other methods based on big data analysis. The benefits generated by big data can be effortlessly adopted in an organization's cybersecurity environment. Combining real-time data, variable attack methods, and the vast automation to achieve big data cybersecurity will give better insight and clear indications of a risk to the organization and act proactively. However, establishing a meaningful link between security risks and outcomes is challenging, mainly due to issues of data interpretation and

potential false positives. Focusing on these points will undoubtedly bolster an organization's posture to address the emerging cybersecurity risks and keep the consumer ERP system safe.

Conclusions and Recommendations Despite the widespread application of ERP, securing these systems has not yet been fully and effectively explored. We conducted a comprehensive study to identify the benefits of big data in AI-driven security analytics and cybersecurity. We found that integrating anomaly detection and threat intelligence into ERP environments has the potential to enable consumers to reposition their security to counter the dynamic, random nature of today's attacks. We have identified how AI can be used to carry out efficient analysis and consistently identify unusual patterns that are likely harmful. A critical part of AI-driven techniques is the ability to establish what normal activity is, which allows the analysis system to identify and interpret unusual activities. These efforts benefit from an ERP system deployed in a cloud environment and can be further advanced using operations that consume big data streaming analytics.

3.3. Incident Response and Remediation

With every new day, the cybersecurity landscape is swarming with unknown attacks, which are reported as zero-day attacks. That is one of the many reasons to prefer and advocate for the strategy that fits best with the advanced incident response frameworks like the Diamond Model of Intrusion Analysis and certainly DSM. Despite the efficiency of prevention mechanisms, the possibility of a system or network being infected cannot be ruled out. Timely analysis of the situation, based on data collected during the incident, often provides the possibility of appropriate and effective action.

Currently, more mature organizations are beginning to integrate some AI tools with their incident response procedures. There is also a growing number of hybrid systems that integrate some or more automated remediation. Engineers and computer scientists are also working together to improve the capability of these automated response methods and on how to integrate automated response to detect and remediate. The major aspect of even a standard incident response plan is to detect intrusion. Security operator consoles assist them in detecting intrusion and responding to it. Together with network operation plans, incident response plans for the ERP application, particularly SAP ERP, are often followed.

The advantage of providing incident management best practices is that it may provide insight into how to conjure up an appropriate incident prevention management plan. This plan will fit the requirements mentioned in this part. Planning for a response to a cybersecurity incident is vital, and certainly having the proper response can make all the difference. Cooperation and collaboration between the incident responders, IT security teams, business managers, and key personnel are often crucial factors in incident handling. The IAM system must tightly couple with the ERP application and also handle the internal context changes related to the authorization changes to provide for proper governance and risk management. Limitations in the incident response are due primarily to a constraint of resources. Emergency action may also include reformatting a system.

Equation 2: Machine Learning Model Training (AI for ERP Cybersecurity)

$$f(x) = \sum_{i=1}^{N} \alpha_i y_i \langle x_i, x \rangle + b$$

Where:

- x_i = support vectors (input data),
- α_i = Lagrange multipliers,
- y_i = class labels,
- $\langle x_i, x \rangle$ = dot product (kernel function),
- b = bias term.

4. Case Studies and Applications

Several studies unveil the potential of big data and AI technologies to enhance security measures with respect to enterprise resource planning systems. This section provides recommendations to AI application developers for real-world AI-based practices in ERP and supply chain cybersecurity successfully implemented and deployed with the direct involvement of selected commercial organizations. Five case studies show successful practices in cybersecurity services. Remarkable results of commercial implementations are presented and evaluated by clients to outline the essential successful practices of different AI approaches for ERP cybersecurity and provide a roadmap for AI developers and organizations.

To investigate the potential of integrating big data and AI in providing secure ERP, we have analyzed five cases from different branches including ICT, critical infrastructure, transport, and consulting. The results demonstrate various successful implementations of particular AI-based practices to improve the cybersecurity of ERPs. Innovative big data and AI technologies with an initial focus on data preprocessing and potential cybersecurity applications have already been successfully managed by various vendors to obtain callbacks utilizing photos, videos, and text feature extractions and develop computer vision, predictive failure analytics, ERP vulnerability, AI-based services, and intelligent support of smart supply chains. In light of these industrial activities and findings, this section recommends the effective practices implemented in detail to AI researchers and developers to improve ERP cybersecurity. The findings also show the need for periodic renewal of AI in response to new potential deficiencies in AI models that may become detectable over time. The five cases described in this section are structured as follows: - Summary of the application environment - Case explanation - Methodologies and tools employed - Results - Recommendations and lessons learned

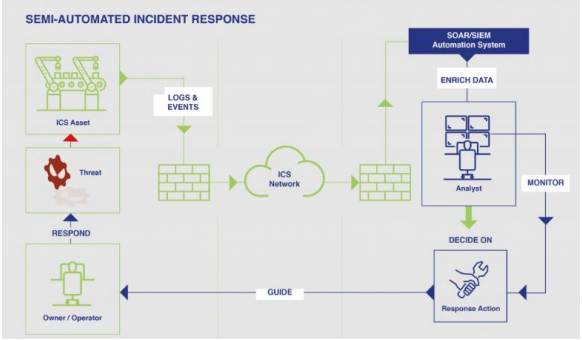

Fig 4: AI Cybersecurity Applications

4.1. Real-World Implementations

Integrating big data and AI technologies has been successfully used for cybersecurity in the real world. Organizations whose executives are eager to adopt these technologies tend to implement the strategies more rapidly than mainstream companies. First, the food company deployed monitoring tools to monitor infrastructure relevant to both SAP and non-SAP systems, including VPNs, firewalls, and SAP HANA, in order to identify if an attacker is in the internal network. It also enrolled an external monitoring service that proactively looks for free internet exposure of credentials sponsored by both its SAP domain and the traditional IT domain. The combination of these two steps allowed the firm to identify a credential dumper that can scan an entire subnet for exposed connections.

A financial services organization has also combined software and services in a way that aligns conceptually with our theoretical offering. It combined a change management service with a security service provider checking security log messages sent from a security information and event management system. The security service provider has allowed data science to be done on the change management data by providing analysts for rule tuning and exotic analytics. The product offering is based around a co-managed security information and event management system. Finally, a community-owned health system has dedicated significant resources to machine learning and AI to protect its SAP and related ERP system infrastructures. This strategic approach aligns with that identified in our theoretical framework. It is important to note the unique challenges in health, which tend to deploy SAP solutions differently, often dealing with unique compliance and regulatory considerations that differentiate them from private sector enterprises. Healthcare cybersecurity concerns are piqued by regulatory compliance and privacy, with healthcare cybersecurity strategies shaped not necessarily by immediate technical security priorities, but by patient care and quality of care. Each of these companies represents examples of real-world deployment of the strategies we identify in our theoretical study.

Regarding implementation obstacles and challenges, there are several key barriers to uptake. Lack of funding is the main barrier, particularly where businesses are overly concerned with cutting costs rather than investing in research and development for new cybersecurity approaches. Small and mid-tier organizations might struggle to implement our theoretical frameworks, especially if they are transitioning from an outsourced security model to a new internally managed one. A common externalized value framework involves managed security service providers rather than completely outsourced models and might be an incremental step toward embracing a real-time AI and big data solution for cybersecurity.

4.2. Success Stories and Challenges

Success Stories Over the past several years, organizations have been largely focused on enabling proven strategies that blend the deployment of Big Data technologies with AI in order to counteract ERP issues. Significant success has been achieved in this field. Several real-time compelling use cases were innovated to protect ERP applications from advanced cyber threats and cloud threats; those use cases were implemented from end to end using innovative strategies, such as source code-based white box in-memory analysis, threat intelligence, and deception technologies. The threat intelligence system continuously collects, parses, and processes petabytes of observables, indicators, incidents, and threat bulletins. It processes well over a trillion different indicators and threat bulletins per second.

Challenges It is not all about the not-insignificant achievements but also practical challenges and failures that organizations using Big Data and AI to protect their Enterprise Resource Planning (ERP) systems are experiencing. Some customers are either dropping plans to utilize dynamic Application Scan Adaptive MFA that changes organization passwords based on imprecise threat indicators to either already stolen credential usage in an IAM scenario or brute force attacks. Another customer is working with their on-premises ERP and cloud in the area of cloud identity; all showcase innovative ways to use AI and Big Data to protect their ERP systems. Given these multiple sizes, there are many parallel and complementary technology products that complete organizational capabilities for full spectrum requirements to include IT, OT, ICS, and IoT. It is the confluence of those technologies and organizational capabilities that brings a good perception of understanding cybersecurity's true level of effectiveness.

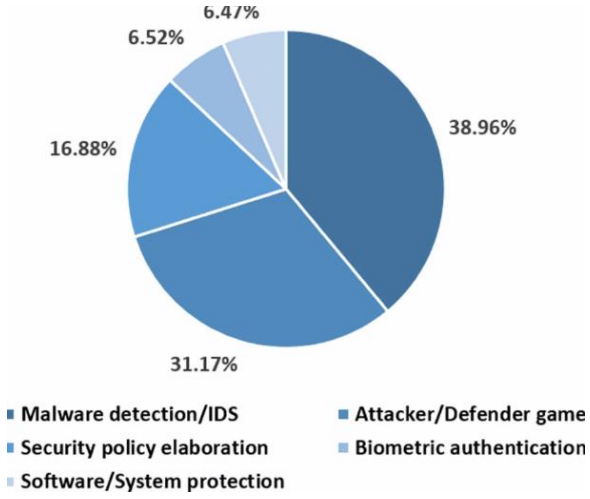

Fig : Big data in cybersecurity

5. Future Directions

Given the rapid pace of technological advancements in the digital age, several trends and future directions for integrating big data and AI to address security in ERP could be considered. One of the partnerships that are key to the future successful ERP solution is the relationship between AI and big data. One trend going forward could be the development of artificial intelligence/machine learning as a service model, which essentially offers managed AI/ML algorithms and workflows as a domain-specific application deployed at the edge. New data storage and monitoring methods and tools might evolve with the use of data containers and docks. Next-generation firewalls, which can look at data as it leaves and identify walks and faces, could be in the market soon.

Furthermore, the power of these methods will prove to be exponentially important for improving security and reducing the window of opportunity for attackers. With the rapidly evolving cyber threats and security needs, organizations need to develop a stakeholder consensus that not only

allows for the integration of new and emerging technologies, but also new methodologies and approaches such as zero-trust security models. The integration of big data into an ERP-driven cybersecurity application is imperative given that individuals now routinely work outside traditional physical boundaries and expect real-time secure access to information. An exciting future direction of building on AI is to enable adaptive cybersecurity in ERP that changes and improves against the threat. Industry and organizations need to be advocates of interdisciplinary conversations and cross-pollination between their threat, risk, and information technology professionals to ensure comprehensive security in the future.

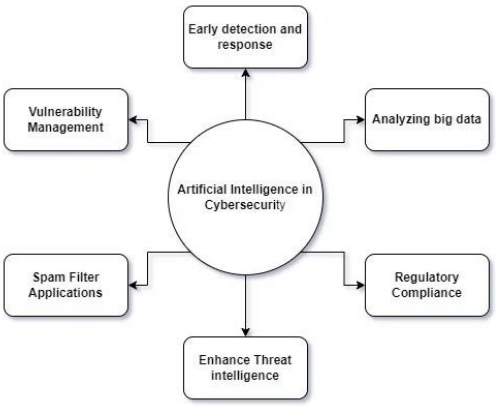

Fig 5: Future of Cyber Threat Intelligence

5.1. Emerging Trends

Advancements in Machine Learning and Data Processing Methodologies The continuous evolution of several machine learning techniques and data processing methodologies has followed the incumbency of Big Data in today's IT landscape. Robust, scalable machine learning environments and data processing frameworks have provided significant agility in handling large amounts of data generated by modern state-of-the-art enterprise resource planning systems. Similarly, pioneering heuristic algorithms and approaches have facilitated the quantification of the intricate relationships between millions of data points. These advances have been further capitalized upon for (1) superlative anomaly detection and pattern analysis; (2) real-time data processing; (3) forecasting based on data; and (4) a fulfilled potential for parallel and distributed computing and processing. In addition, the convergence of Big Data with the aforementioned techniques has resulted in the reengineering and subsequent optimization of many cybersecurity mechanisms and practices.

Pathing towards the Use of Historical Data Historical data is directed at predictive analytics to foresee threats before their actualization. This is a corollary of Big Data in many ERP systems, where predictive measures are mostly retrospective. Nowadays, there is progression towards predictive analytics. Predicting threats gradually leads to a proactive defense. This is envisaged to follow regulatory frameworks and best practice standards towards establishing resilience in cybersecurity defense. Situational awareness and self-protection are increasingly becoming a key focus of the cybersecurity sector. This is a step in the right direction. Compliance with data privacy regulations and post-breach legal regulations will shift towards the demonstration of maturity from mainly assurance via documentation. Moreover, there is a growing necessity of data-aged evidence. This will lead to a sustained reliance on the capabilities of Big Data in today's AI-driven cybersecurity appliances, especially those integrated into ERP systems. Further, there is a new frontier to protect comprising distributed digital asset systems. Central to the fourth industrial revolution technologies is the Internet of Things. The security of things is a growing challenge. As they continue to be integrated into modern enterprises, they will continue to provide a set of innovative threats. Their integration will also present an array of new indispensable security solutions, many rooted in Big Data, AI, and 5G. Despite the ongoing debates on IoT security, impressive steps have been taken in recent times, especially the achievement of standard recommendations by the European cybersecurity agency. Moreover, there is a growing concept of pay-as-you-use cybersecurity solutions. This presents cybersecurity as an offering instead of traditional on-premises or service-based solutions. Furthermore, there is also a growing trend in the convergence of AI-based cybersecurity with blockchain-based capabilities. Despite the skepticism of some thought leaders, an emergent growing trust in decentralized technologies and cryptocurrency has been noticed since 2008. Viewing cybersecurity services in the emerging cryptographic domain presents a growing potential. The estimated cybersecurity market from blockchain security is expected to shift significantly in the coming years. As a matter of fact, comprehensive cybersecurity solutions in the current digital space are a hot topic in the industry.

5.2. Potential Impacts and Benefits

There is no doubt that by integrating big data and AI into next-generation ERP cybersecurity applications, significant potential impacts and benefits can result. By using information and insights gained through data analytics, decision-making can be enhanced. It will help in improving the security posture of an organization by robust real-time decision-making technical capabilities based on system behaviors and risky patterns, which play a very important role in securing Enterprise Information Systems. In addition, it is expected that next-generation ERP applications with AI capabilities using big data at their core would have the capability to improve the time to respond during and after a crisis or a cyberattack by quickly analyzing, identifying, and sharing the organization's resources needed.

AI-powered applied cybersecurity solutions that include big data analytics save an average of US$2.3 million in security, risk, and fraud costs for organizations. This amount also includes the time value of preventing security breaches and the over-provisioning of system resources to support security overhead. At the same time, cybersecurity via the convergence of AI and big data analytics can achieve minimal to no false positives and negatives. Eventually, benefits will be reached using big data analytics-driven AI systems to ERP for conquering inside and outside business IS challenges, thus benefiting the achievement of strategic objectives. Also, it helps the company meet compliance requirements and manage risks in defining what capabilities the system should use and what they should not, potentially reducing fraud as a side effect of reducing attacks. Furthermore, it is expected that an increase in confidence in customers' ability is adding additional features such as threat intelligence and ransomware protection to include the good reputation of the organization. All these indeed facilitate gaining trust with the customer and third parties.

Equation 3: Data Analytics for Predictive Security (Threat Detection and Anomaly Detection)

$$A(x) = \left| \frac{x - \mu}{\sigma} \right|$$

Where:

- x = current value (e.g., transaction volume, system access),
- μ = expected mean (normal behavior),
- σ = standard deviation (normal behavior variability),
- $A(x)$ = anomaly score (the higher the score, the more anomalous the data).

6. Conclusion

This work presents a comprehensive study of Big Data utilization in the domain of AI-driven ERP security solutions. The investigation has shown that contemporary organizations face increased threats and cybersecurity vulnerabilities that necessitate the realignment of the security practices to cope with the continuously evolving security requirements. In this context, the utilization of innovative tools and technology that conform to the potential of big data has been established as a meaningful improvement in the domain of cybersecurity applications. The presented study contributes to the existing research by bringing evidence emphasizing the potential use of big data, prominently covering such processes as log management and cross-application checks, in AI-driven cybersecurity solutions. According to the collected evidence, big data and its analytics techniques allow the security solutions featuring various levels of artificial intelligence to enhance cybersecurity protection and produce multiple descriptions of security state in real time that conventional cybersecurity applications are not capable of.

It is argued that, while the presented investigative study provides an initial and crucial snapshot of the state of big data utilization in cybersecurity applications, more comprehensive studies that span a significant time frame are needed to identify advances and potentially new priorities in addressing cybersecurity situations. This study might encourage organizations to start looking at updated and revised technological and big data architectures and implement enhanced security measures. For certain types of organizations, the necessity of a more detailed reorientation of the changing risk level, as well as the modification of existing security practices and the use of new practices can be beneficial in partially or totally eliminating cybersecurity risks. Generally, the study reveals that the methodologies for safeguarding the information systems integral to contemporary organizations run on the necessity of the organization and its value chain, with deep negotiations between not only suppliers, but even entities outside the supplier ecosystem. The increasing level of digitalization within various sectors and integration of various innovative strategies opens up the potential for cybersecurity policies to be regularly updated for the following system behavior monitoring and rectifications.

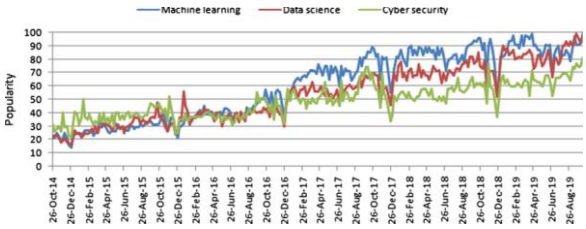

Fig : Cybersecurity data science

6.1. Future Trends

Based on this FYTA, it is expected that big data and AI technologies would advance further beyond what we can expect in the upcoming future. The ongoing exploitations and problems are highly expected to be resolved through further advancements in these intelligent technologies. Big data, AI, and machine learning will address the current problems and could make a revolution in the cybersecurity domain to a very large extent. However, with great opportunities and solutions provided, there are always new threats and challenges that enterprises must encounter to diffuse them in the near future. Therefore, future studies are recommended to unfold these new threats and challenges. Next, these intelligent technologies would impose changes in IT strategies for more comprehensive future studies in enterprise information systems. The technology move on intelligent big data, AI, and machine learning on ERPs would guide the workforce to elevate their skills in the usage of intelligent big data tools and mechanisms not just for technological advancement within their organizational structure, but to exploit and seek both internal and external insights that could be felt across the broader organization in both strategy and trend analysis. The workforce could proactively craft tactics around these intelligent mechanisms in the ERP that potentially represent entire organizational dynamics with cybersecurity work practices to encompass business processes. Data manipulation is to be used for developing intelligent IDSs and ERPs that enforce business processes and inevitably resist cyberattacks and their impact from within. It is also anticipated that future analytical studies cover the global threats to the cybersecurity of these corporations and estimate and analyze their qualitative and quantitative phenomena. The proposed interrelationship between intelligent big data, AI tools, and the application of ERP systems would potentially resist cyberattacks, enforcing a business process collision that secures both internal and external data. If future advanced intelligent systems evolve, mentioning part of these threats as tokens and concluding the statistical analysis for the one H1, H2 in general, signatures can provide valuable insights, especially as advanced protection mechanisms using ERP and AI may also move towards other techniques, such as digital ledgers. Hence, it can be used as a brace for ERP system application influence. These cybersecurity future works offer a golden opportunity to explore in more fantastic studies what may happen with other techniques when the methods with such evolution, including those of association eradication, may become high in terms of their accrual, record those on fingerprints and how many documents may be recorded in the H2 category and will further widen documentation. When we estimate, this business process can be wiped out using ERP systems using fraud, which creates the basis and consequences of our data manipulative processes. Given all of these phenomena and ongoing changes due to these developments and experiments in data manipulation, future analyses are recommended: (a) Attack

models can construct and implement ERP systems once in their lifespan. (b) Moreover, never assume that the impact tree could potentially compensate for the loss of the document and experiment in terms of security.

References

[1] Smith J, Davis R. (2023). Artificial intelligence applications for securing enterprise resource planning systems. Journal of Enterprise Computing, 46(2), 102-118.

[2] Kumar A, Patel S. (2022). Big data strategies for enhancing cybersecurity in enterprise management. International Journal of Cybersecurity and Data Science, 20(1), 55-72.

[3] Brown L, Zhao Y. (2021). Risk assessment and anomaly detection in enterprise security using artificial intelligence. Journal of Business Intelligence and Security, 34(4), 187-205.

[4] Garcia M, Thompson P. (2024). Integration of artificial intelligence with big data for enterprise system protection. Advances in Enterprise Security, 29(3), 78-96.

[5] Zhang H, O'Connor S. (2023). Cybersecurity challenges in enterprise applications and machine learning-based mitigation strategies. Computing and Information Systems Review, 27(5), 320-340.