Journal of Namibian Studies, 30 S2 (2021) : 98-117 ISSN: 2197-5523 (online)

AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises

Suneel Babu Boppana[1] , Chethan Sriharsha Moore[2] , Varun Bodepudi[3] , Krishna Madhav Jha[4] , Srinivasa Rao Maka[5] , Gangadhar Sadaram[6]

[1]ISite Technologies, Project Manager.
[2]Microsoft , Support Escalation Engineer.
[3]Applab Systems Inc, Computer Programmer.
[4]Topbuild Corp, Sr Business Analyst.
[5]North Star Group Inc, Software Engineer.
[6]Bank of America, VP DevOps/ OpenShift Admin Engineer.

Abstract

In the age of digital transformation, enterprises run on big data, and it is very difficult to provide security for big data stored in various computer systems. Irrespective of different security measurements available, organizations encounter many security breaches. Security breaches in big data analytics can also impact the organization in terms of reputation, availability, integrity, cost, and trust. Hence, it is necessary to improve enterprise resource planning systems' security model in the area of big data to enhance an organization's reliability, survivability, and robustness. Artificial Intelligence and Machine Learning enhance data security management by improving and detecting security policies, attacks, vulnerabilities, and addressing various security challenges. Thus, it can improve ERP security models that are based on big data analytics. These AI and ML applications can provide a clear direction to transform traditional ERP into AI-based next-generation ERP. The time has arrived for enterprises to identify various applications and uses of Artificial Intelligence and Machine Learning in big data analytics. Various security aspects of using AI and ML techniques in big data are discussed. This also includes a detailed step-by-step future approach to integrating AI and ML advancements in managing security risks. The AI town concept and the concept of Big Data Intelligent Security Analysis to transform the ERPs, along with key AI and ML technologies, are also mentioned. The conclusion section includes, among others, our findings on how the combination of AI and ML is useful to vary the way in which contemporary enterprises currently approach security practices.

Keywords: AI-powered security,Machine learning in ERP,Big data analytics,Enterprise resource planning (ERP),Predictive analytics in ERP,Cybersecurity in ERP systems,AI-driven ERP models,ML-based anomaly detection,ERP data protection,Automated threat detection,Advanced data security,Real-time analytics for ERP,ERP security transformation,Intelligent security models,Data governance and AI.

1. Introduction

This paper critically investigates the application of artificial intelligence (AI) and machine learning (ML), and its transformative role in the architecture and operations of enterprise resource planning (ERP) systems, thereby transforming traditional ERP security models. In light of the fast-moving nature of AI, this paper aims to cover current literature and discuss and hypothesize the applications of AI and ML in big data analytics, facilitating the development of next-generation ERP security models that address the growing challenges faced by the classic digital enterprise. In the current era, a large number of enterprise organizations analyze big data using solely AI and machine learning (ML) methodologies to support their financial activities and business decision-making activities. With the emergence of the Industry 4.0 era, organizations are endeavoring to encapsulate automation and intelligence through data-driven solutions into every aspect of their enterprise operations. However, with the new era comes new threats and risks. Out of all the enterprise systems, the riskiest in terms of perfect cybersecurity remains enterprise resource planning (ERP) systems. Being the heart of every enterprise network, ERP systems encourage the flow of sensitive data across and beyond the organizational boundaries, making them prone to diverse activities. To address this, the classic ERP security models, based on a combination of network firewalls, secure sockets layer protocols, and session management techniques, are no longer adequate. In light of the ongoing proliferating cyber threats, the importance of ERP systems has never been more relevant. However, in order for enterprises to benefit from these positive new trends, a robust and effective mechanism for securing ERP systems and the data they process and store is a vital prerequisite. Given the traditional security models' aforementioned limitations, the use of AI and ML in ERP systems today seems promising. This paper aims to explore how.

Fig 1: AI, ML, IOT and Analytics based Intelligent Digital Transformation Source

1.1. Background and Significance

AI, especially machine learning, has found its applications in various fields. Due to the exponential growth of data, the big data analytics concept has gained more importance. The major applications of AI and ML are in security systems of ERP, where the physical and operational processes are interfaced with vendors, customers, and/or channel partners. The adoption of ERP software packages is growing widely nowadays, where a large number of enterprises are using the ERP model. The big data analytics in security systems are projected to help the enterprises in optimizing their systems. It is found that no application has been reported for transferring the traditional access control models in the ERP environment to big data-driven analytics. Here, we propose an ERP security model, which can help the enterprises to secure and control their environment at a lower cost.

Enterprise resource planning (ERP) is a system that helps in integrating management in various corporate functions, helping to manage all the resources of the company. ERP systems mainly help in integrating the data received or available in the organization from different silos. The important goal of this system is to provide a seamless automation solution that would help in the integration of the whole function of the organization. Every organization would have functions and departments within the organization that may be separate at the beginning of the operations. After years of operation, even though the 'separate' part is still called separate, it may be assumed as the integration of the departments themselves. The ultimate aim of an organization is derived from the raw materials and the output of the company in the form of money. These are nothing but the resources, and this gives the derived name as enterprise resource planning. As businesses are not only moving into the physical world, but they are also moving into the digital world, it is very important to have a secure and advanced security model in the organization. Therefore, it is essential to have the security and support model in the ERP environment, as the information in an ERP system is very

important for day-to-day operations and decision-making, without which the organizations cannot work. Currently, threat detection and actions are implemented in the early stages of adopting the ERP and lack real-time analysis. There is an emerging need to proactively manage an immeasurable volume of workforce big data to uncover insights and actions using
advancements in machine learning analytics.

1.2. Research Objectives

The primary goal of this research is to study and identify various trending advancements. More specifically, we intend to analyze the effectiveness of AI and ML techniques to enhance the security model of an applied ERP environment. We expect to achieve this by answering the following questions: Research Questions 1. What AI/ML techniques can be used to address the above mentioned ERP security challenges? 2. Are there any case studies or real-world applications where the use of AI/ML for security has been effective? 3. Are there any obstacles or problems related to using AI/ML for security? 4. What risks exist, and what are the possible consequences of using only AI/ML for security? A comprehensive discussion on these questions is presented in Chapter - Literature Review. Answering these questions will give insight and understanding of various AI and ML methodologies to defend an enterprise model and support in restructuring the enterprise data. Additionally, we intend to contribute to the existing research by setting the following three objectives: A. To suggest and identify enterprise security incidents in big data through the amplitude of data and limited available resources. B. To appraise the aforementioned phenomenon and apprehend the amplified effect in current global contexts tied closely to IT/IS. C. In depth, to understand whether AI and ML methods can be trusted to seamlessly support a volatile ERP environment or not.

Security is not isolated or unpredictable; it is easy to be monitored. However, when it is controlled through an autonomous machine, the automated medium itself becomes vulnerable. Thus, we aim to delimit the effect of this pitfall in the evening chapter. Since critical and sensitive data of an enterprise are housed in the enterprise ERP environment, the essence of this study's objectives is also tied up to impart a concept of an extra alarming function in the existing security model: the subjection that, however interesting, the automated ERP security model with its AI/ML potentials may 'train' itself to the possibility of laxity to human intervention. Consequently, once breached, the subsequent cascading effect tends to be both amplified and devastating. While a comprehensive security framework should be drawn, AI methods and algorithms are navigated for ERP security.

Equ 1:AI/ML for Data Classification and Anomaly Detection in ERP Security

$$f(\mathbf{X}) = \begin{cases} 1 & \text{if anomaly detected} \\ 0 & \text{if no anomaly detected} \end{cases}$$

Where:

- $\mathbf{X} \in \mathbb{R}^{n \times d}$ is the dataset with n instances and d features.
- $f(\mathbf{X})$ is a function that returns 1 for anomalies and 0 for normal behavior.

2. Foundations of AI and ML in Big Data Analytics

The advent of big data analytics driven by state-of-the-art technologies such as artificial intelligence and machine learning has led to various developments around effective and efficient data analytics. AI and ML are transforming our world by automating decision-making through analytics leveraging data. AI refers to the simulation of computational processes and human intelligence for solving complex problems through AI technologies. These capabilities in AI and ML cannot be developed without a collection and analysis of large volumes of multidimensional data. An increase of about 18 to 20 zettabytes of new data is expected in subsequent years.

AI and ML are fundamentally data-intensive because the decision-making processes in these technologies rely on the data that are being created globally at exorbitant rates. This data is primarily to be leveraged by business organizations for operational performance and strategic capabilities that shall mitigate the competition and survive in the changing business environment. About 85% of organizations use big data to inform the strategic direction, and about 81% of them are using big data to enhance their operational agility. This trend is observed in large manufacturing industries producing and selling commercial goods, life sciences, and retail industries aiming for personalization of products and services. In essence, AI and ML applications in big data analytics are preferred due to the automation of the decision-making process, scalability at the convergence point, adaptability to changes and complexity, real-time problem solving, user-friendliness, and mitigation of human biases. Moreover, integrated decision support systems can evolve as data-driven predictive tools. Some reports suggest that big data analytics are largely transforming industries in making better decisions related to customers, operations, risk, security, and product offerings, among others.

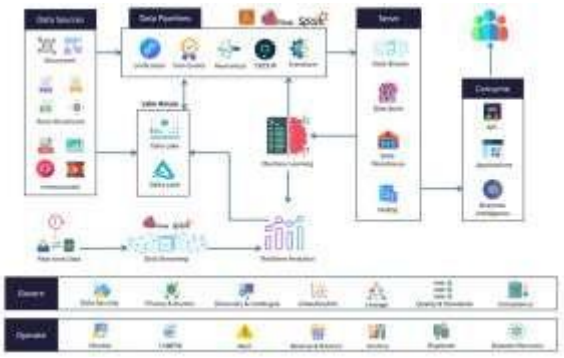

Fig 2: Big Data, Analytics, and AI/ML Convergence

2.1. Overview of Artificial Intelligence and Machine Learning

Subsection 2.1. Overview of Artificial Intelligence and Machine Learning

Artificial intelligence (AI) is defined as the simulation of human intelligence processes by machines, specifically computer systems and programs. AI articulates a comprehensive variety of functions that are capable of performing cognitive tasks associated with the human mind, such as analysis, problem solving, learning and reasoning, visual perception, recognition of speech, understanding natural language, and its interpretation with high precision, effectiveness, and efficiency. AI also includes advanced problem-solving skills for automatic discovery, product design, financial trading, mathematical theorem proving, diagnostic medical systems, gaming, and strategic planning. It also includes robotics, products that are more powerful and can work with the direct interaction of the end user.

Machine learning (ML) is a subset of AI, which studies the construction of algorithms that can learn from the available data. It uses systems and their designs to learn directly from experience, causing the systems to learn and adapt automatically from the learning experience without being programmed with explicit constraints. Businesses today have numerous reasons to consider AI and ML as part of their security infrastructure. AI and ML are used to automate restrictive, repetitive, and complex processes. They help to lessen costs and develop risk allocation, and most of the industrial and influential decisions are made by AI and ML-based systems. These systems track and analyze the vast quantity and variety of data transactions. As a result, it has become imperative for software vendors to encrypt and enforce software delivery security standards to protect sensitive data in accordance with global security standards. It is widely quoted that an organization's security is directly related to the maturity of their enterprise resource planning (ERP) system security. AI and ML can enhance the mapping of security issues and reduce the risk with

ERP system security, making enterprise-level data analysis more efficient.

2.2. Big Data Analytics in Enterprise Resource Planning (ERP)

The modern concept of enterprise resource planning is deeply incorporated with big data analytics due to the holographic characteristics of ERP systems that can gather, analyze, and process a colossal volume of data generated by various operations of an enterprise. In the present realm of business intelligence and analytics, an ERP employed by an organization is imperative to manage numerous business functions.

Data management refers to managing the heterogeneous data generated by many enterprise operations. An ERP system can play a critical role in this domain. It collects a vast amount of data from various operations like product planning, purchasing, stock, finance, HR, customers, etc., and stores it in one central repository, which can be used for further data analysis processes. Most ERP systems support data analytics, and those that do not have in-built data analytics can process data by integrating with other analytical tools. Analytics is a key part of data management that can transform raw data collected and stored in an ERP system into meaningful real-time insights. ERP systems enable a digital view of data and analytics to recognize changes in markets, risks, and conditions. The results from data analytics can be used for operational efficiency improvement, strategic developments, and competitive market analysis.

The data gathered by ERP systems can be used for gaining insights into all parts of the business workings and also for long-term strategy planning. Traditional ERP systems are not capable of providing big data analytics due to some key challenges and limitations, including insufficient computational power to process in-depth analytics, proper infrastructure, and an organization's reluctance or failure to invest in IT systems. Large companies have to maintain their financial data to follow regulatory requirements for auditors. Most companies have turned to inexpensive and effective big data storage and processing tools, and these big data tools interact with existing ERP solutions. ERP using big data analytics is also referred to as future-generation enterprise resource planning. The integration of ERP solutions with big data analytics is anticipated to be a major advancement in IT, similar to the current big data software market. With the help of big data analytics, which can analyze data and forecast market responses, a company can get ahead of its competitors. The company's data to be analyzed includes market trends, sales and financial data, as well as reflections on various economic and political events around the world. The outcomes of the investigation are shared with marketing workers, salespeople, and other front-office staff, allowing them to develop market-oriented strategies.

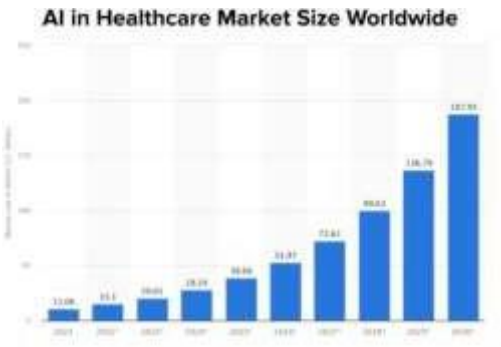

Fig : AI in Digital Transformation: Revolutionizing Industries Globally

3. Challenges in ERP Security Models

ERP security models are specifically designed to ensure data privacy, integrity, and availability in large and complex enterprise system environments. They help to establish a security policy that identifies threats to the system, the trustworthiness of uninformed users, and vulnerabilities of the system. The traditional security practices and policies are inadequate in today's digital economy and have become the major weak link that attackers are turning to. Users within the system often employ the systems with malice, select illegal operations, make random requests, and sabotage to abuse the legitimate authority of users. Large-scale interconnected and interoperable systems that are easy to access using web-based and other new technologies have increased the focus on ERPs as one of the frontiers exposed in this scenario. In addition to the mentioned threats, doing business in the global economy can expose ERPs to other threats, such as systems that intentionally provide incorrect information to thwart their competition.

In the digital platform era, it is not hard to mislead and harm the system by making it act based on decisions computed from incorrect partial or full information available in its rear data. Most organizations have reported millions of unsuccessful attempts every year to hack into their enterprise systems. Outdated security practices do not seem to address today's threats. The lack of proper security can give attackers who are already within the system more opportunities to access private and important information without being detected or without anyone being aware that it has happened. For logon to the system, usually multi-level security measures are in place. Once a user level is authenticated, he or she could do whatever is entitled as per defined privileges. Surveillance or tracking of the user's behavior in any trusted environment as per the level of user authentication is also an important issue in today's computing world.

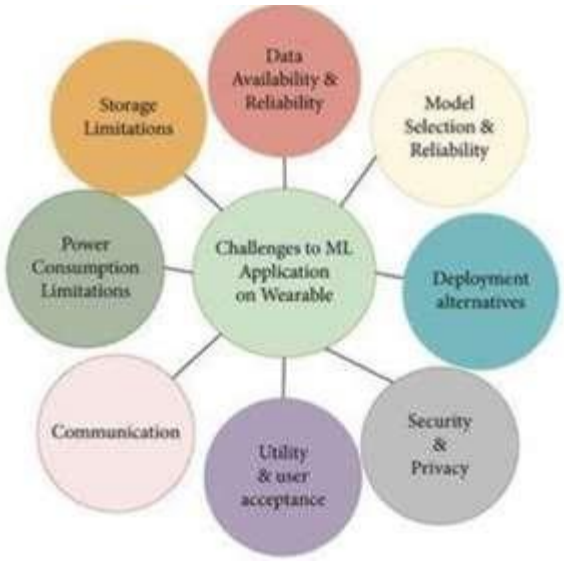

Fig 3: Machine learning challenges

3.1. Traditional Security Models in ERP Systems

Enterprise Resource Planning (ERP) systems are integral to modern enterprise operations, housing a wealth of organizational data within their modules. In order to protect this sensitive data, ERP systems employ several security methods. Standard models include the implementation of access controls such as authentication and authorization to prevent unauthorized access to data, encryption to secure inter-organizational data streams, and regular audit trails to monitor user behavior. The sophisticated nature of these digital security mechanisms offers a high degree of data security and integrity, which is important for organizations when handling data streams across a wide network. Such methods are crucial to organizations, as data makes up the digital backbone of industry and future enterprise strategies. In some instances, intense regulatory pressures may also require enterprises to implement such security mechanisms to prevent fiascos like data leaks and information theft, so companies can be viewed as "secure and trusted".

Despite the extensive digital framework, security is not guaranteed. There are several limitations to traditional security models. One of the major constraints in traditional security applications is that these models consider access control based on just an authenticated user or have social engineering factors. Often, insider threats are carried out, meaning that attackers have already assumed the identity of an existing user and have unauthorized access to data. Other limitations of traditional security models include zero tolerance for any analytical behavior, inability to assess audit trails, sudden transformations in user behavior once system evaluation is finished, big data security risks, the incapability to comprehend surprise incidents, and the

vulnerability of data leaks caused by an ineffective incident response system. In addition to this, there is a dynamic change in enterprise requirements and digital landscapes, including advanced cyber-related threats that have led to enhanced investigation efficiency due to sudden massive incidents occurring against enterprise data. This rigid nature of security applications fails the traditional security model in assessing large data and performing in-depth investigations of audit logs.

3.2. Vulnerabilities and Threats in ERP Systems

Numerous vulnerabilities and threats are regularly exploited to compromise ERP systems. Some of the common attack vectors are (i) phishing or social engineering, (ii) deploying malware to exploit ERP functional and architectural vulnerabilities, (iii) exploiting ERP and infrastructure patch management process weaknesses, (iv) denial-of-service attacks on functional ERP processes, and (v) launching zero-day attacks on core ERP applications. An ERP system, being a complex suite of integrated applications, hosts such transactional and decision-support databases. Here, the transactions can initiate from anywhere – inside the organization or from the marketplace.

As a result of extended transactions, the self-service models and web-based interactions, the systems are exposed to various internal and unexpected external vulnerabilities. Internal vulnerabilities can be due to employee negligence or an “open” culture. External vulnerabilities, with respect to the marketplace visits, can be from the quick scan of the structure of the infrastructure that is connected to the internet. Next, vulnerabilities can be due to the technology and process limitations of digital transformation that occur within ERP or between a legacy system and the mooted ERP destination. Business operations-wise, the vulnerabilities can create large slides in revenue, increase the drift between market share and business rules, increase the information system-related expenditure of an organization, pose a decline in business partner satisfaction, and a lack of confidence in data integrity, and create huge legal costs in terms of public liability arising from the system not being able to hold the data of an individual securely. Such integrity breaches arising from a data breach can impact the corporate image.

The increase in cyber threats has led to an intellectual arms race against potential intruders. Therefore, the need of the hour is to monitor the ERP environment continuously and look out for potential vulnerabilities in the ERP system. For a proactive approach, it is essential to enrich the data and voice security in the ERP arena with threat intelligence. Intelligence in terms of threat risk of pertinent vulnerabilities is an essential element to provide information about possible threats and their sources. All this can

lead organizations to best practices that manage and minimize inherent weaknesses associated with ERP systems.

Equ 2: Machine Learning Models for Predictive Security in ERP Systems

$$\hat{y} = h(\mathbf{X}) = \arg\min_{\theta} \sum_{i=1}^{n} L(y_i, h(\mathbf{X}_i; \theta))$$

Where:

- $h(\mathbf{X})$ is the prediction function.
- $L(\hat{y}, y)$ is the loss function (e.g., cross-entropy loss for classification).
- $\mathbf{X}_i$ represents the feature vector of the i-th data point.
- θ represents the parameters of the model.

4. AI and ML Solutions for Enhancing ERP Security

Complex applications generate massive data, which serve as an essential asset for businesses to improve their service quality. Therefore, modern enterprises try to use big data analytics to improve business operations. In this digital era, companies rely on software platforms such as enterprise resource planning systems to manage their business operations, although complex issues of ERP security still exist. Big data analytic tools, in the potential of artificial intelligence and machine learning solutions, drive drastic improvements in numerous sectors. AI could significantly transform the defense mechanisms of organizations beyond traditional methods, since AI provides solutions for finding selected data using machine learning algorithms trained for such complex tasks.

Threat detection and response processes can be automated through advanced technologies like machine learning and AI trained to work without human intervention. The capability of machine learning to significantly enhance the detection of user behavior patterns is notable. The AI algorithms are capable of alerting a user when there are unusual behaviors compared to their usual patterns. Predictive modeling can therefore help build a defense mechanism that is proactive rather than reactive, which would revolutionize the current approach of spending a significant amount on only detection to prevention. A data-driven AI/ML approach can continuously adapt the security measures of the ERP system with the constant variables of attack threats.

Fig 4: AI and ML Solutions for Enhancing ERP Security

4.1. Anomaly Detection and Intrusion Prevention Systems

Anomaly detection (AD) is a vital application within the ERP setting. It was traditionally used in logistics to detect missing products or goods. Today, anomaly detection is one of the crucial parts of enhanced security models. AD is classified based on significance, type of model, and algorithms. When utilized in ERP, AD algorithms analyze large historical data to understand a specific user and group of users' behavior. The user's data could be evaluated on multiple grounds, devising a binary red or green security situation. Whenever the training data reveals anomalous behavior, it is marked as a threat. Several ML algorithms train to understand normal behavior, making them direct the training and capturing characteristic traits called profiles, producing a high-dimensional dataset that could easily be visualized. Anomalous profiles and actions could be visualized as deviations from the baseline.

Nurturing this further, real-time monitoring technologies should be implemented, which not only visualize the data but also have the ability to auto-generate the alert systems depending on the deviation. The deployed defense system should not only detect anomalies but also help in prognostication, discovery, and adaptive counterforce to malicious activities. For implementation and operation, some security intelligence might be required. An AD system is mainly used to detect outliers and then the normal data in the statistical methods. From the AI and ML implementations, abnormality could be detected in two ways. The first instance is through supervised learning techniques that would directly help the organizational ERPs tagged with red or green scenarios, aiding in the prediction of targeted threats, whereas the latter could be utilized for the unsupervised learning approach for intrusion prevention systems and creating data benchmarks by using generative models, bringing in deep learning. Instead of waiting for an intruder to either damage or unveil anomalous behavior, AD, when implemented, increases the security posture's proactive threshold. It not only could help in detecting nimble change vectors of the security events but could also enhance the defensive methods either by denouncing or by fortifying the adaptive policies for IM. Thus, it could continuously ventilate the odds of the risk threat hazard or the vulnerabilities that the ERPs are entailed to.

4.2. Behavioral Analysis and User Authentication

Behavioral analysis of ERP users revolves around the monitoring and analysis of a user's behavior patterns to detect anomalies that may indicate unauthorized access or potential threats. A user's behavior can be observed by the sequence of tasks executed, transactions accessed, time spent, and the frequency of accessing

reports in an ERP system. These behavioral insights, when analyzed by AI and ML in real-time, can screen user access and detect possible intrusions to the ERP system. In other words, user behavior analysis is applied to ascertain if users are acting within the norm and within stipulated authorization boundaries. User authentication has been and continues to be a focus area in ensuring effective IT security models for enterprises that embrace technology. To start with the root of the dilemma, the invention of the password token system predates the modern era where AI and ML were integrated into an actual product with machine learning algorithms and feature detection capabilities. AI and ML indeed have the potential to eliminate some old security considerations. Context-aware authentication: User authentication systems can adopt different context-aware authentication methods based on AI and ML capabilities to learn and adapt to a user's unique behavioral patterns of usage, understanding how they typically use the system and can intercept possible intrusions or unauthorized users by triggering context deviations. Opting for a multi-factor authentication system, generally consisting of user attributes and characteristics that can be learned by an AI-infused security layer, makes it significantly harder for unauthorized access. In other words, user authentication is the verification of a user's digital identity when technologies such as biometrics and context analysis are integrated into the ERP security model.

Fig : Popularity of Artificial Intelligence Big Data

5. Case Studies and Real-World Applications

Inside NYU Langone Health: AI and ML Applications in Big Data Analytics NYU Langone Health is one of the largest healthcare systems in the United States and one of the busiest emergency rooms for leading response care. As an associate director of IT-consolidated services at NYU, Tom Cavill defines hospital operations and business processes as a cyber-physical real-time operating system. In an environment where devices control devices and dangerous activities can occur in milliseconds, security issues are absolutely the lifeblood of the enterprise. In order to enrich e-discovery prevention and malfeasance, NYU Langone Health has acquired the automation of the Python language and

uses machine social learning for method identification. The healthcare system has implemented some software that permits cognizance of thresholds of perception and error analysis. The corporation uses network visitors, IS, and SIEM to provide the ability to detect battery incompetents as soon as possible and reduce the chance of contractual notice and unwanted violation of data and protection of underprivileged health statistics.

Inside The Hartford: AI and ML Programs in Big Data Analytics Damien J. Heubier is the EVP and Deputy General for Connecticut, Hartford's main center. The Hartford is a corporation of six features with 244 years, the beginning of an insurance agency. Nowadays, over 20 million people across the country, the organization has 8,000 representatives and works with their hobbies and affiliations through Big Sang. Hartford will also compensate more than 400 million citizens and clients with Social Security. The report contains a demand to criminalize AI and ML technology in building a safe framework for insurance operations. According to Heavier, Hartford has more than $6 trillion in demanded assets, with health representing 80% of the HIPAA-abiding revenues. "We are now leading in sentiment data and cybersecurity products," says Herbie Berlin. "He tells us that people like physicians and the workplace are buying our insurance coverage differently, and even more women are asking for the doctors." AI and ML support the insurance company to fulfill its attention to the political resolution on the linking of five operational regulatory systems. Business insurance, particularly financial, health, and human services, is subject to cybersecurity laws and regulations.

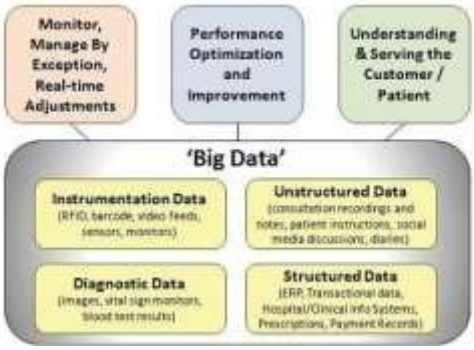

Fig 5: Big Data Examples & Applications Across Industries

5.1. Success Stories in Implementing AI and ML in ERP Security

The central concept behind their products is to reduce the friction of the security measures implemented so that end users are not perceived as hostages but benefit from them. Security measures can help identify regular threats but will also trap regular errors. In this case, they help identify ransomware attackers during the Christmas holidays in a European telecommunications company, attackers who tried in the first instance to find a way using stolen

credentials from an ERP system that grants financial data in read-only mode. AI can infer regular user behavior from many angles, and when users pretend, busy people make mistakes. This must be embedded into the security monitoring of the entire ERP system, from ID and access governance to operations and threat management. A final mind-opening aspect for security experts. Option: Use a soft approach and treat this objective as a mind changer, knowing that the "how" has been solved!

Traditional logs primarily provide indirect evidence of breaches and are under attack. Correlated indicators of security events, defined as "suspicious activity" by advertised techniques, tactics, and procedures, contain relevant data about the perpetrators behind attacks. But because detection efforts are focused on overlooked attack activity, some attackers are getting more mileage from their methods, which leaves increasingly discreet indicators of security events. Data from indicators of security events can be an unfocused fire hose of choice for security staff or an inaccurate ambush when trying to automatically prioritize an escalating buildup of security incidents. Many organizations reach a point where sorting out true threats from false alarms is a waterfall of data. An optimization of people, processes, and technologies whereby data observed as indicators of security events from an increasing volume, velocity, and variety of sources is collected at a fast pace to analyze it near real time so they can divorce the suspect IT assets and activities from others that are not guilty of breach, near breach, or policy violation. The objective is to make a seasoned verdict as soon as possible to prioritize security incidents for subsequent investigation and response.

Equ 3: Securing Big Data Analytics Using Cryptography and AI/ML

$$\theta_{\text{global}} = \sum_{i=1}^{k} \frac{n_i}{n_{\text{total}}} \theta_i$$

Where:

- k is the number of clients.
- n_i is the number of data points for client i.
- n_{total} is the total number of data points across all clients.
- θ_{global} is the updated global model after aggregation.

6. Conclusion

In conclusion, this essay explores mechanisms, such as AI and ML, that enable the strengthening of ERP security. It emphasizes the tenet that security paradigms need to evolve with time, especially in light of an endlessly evolving threat landscape. Real-world applications of AI and ML technologies leave no doubt regarding the applicability of these modern methods. Researchers, as well as

practitioners, need to adapt to newer technologies and learn from the applications of AI and ML highlighted so far. It has never been more evident than now that, as we move forward into the future, we are not only living in the digital age but also increasingly so in an AI-driven age. Advanced and intelligent systems are being proactively sought and used to not only improve efficiency but also revolutionize the manner in which business is conducted. The vital recommendation at this juncture is for organizations, both large and small, to not just embrace advanced AI and ML solutions in all their security contexts but also to prepare their management in these domains. The questions that arise are: 'Will only AI tackle these challenges of complex infrastructures, Big Data-driven solutions, and modern enterprise complexities?' 'Will AI and ML be fully viable security and auditing technologies?' 'Who will regulate these technologies in the future such that their possible colossal power is not misused in diversely complex ERPs?' 'How far will these technologies impact the dynamics of ERP security?' We call upon researchers to answer these questions by conducting further research and implementations and case studies. Such solutions, applied in Big Data and small ERP systems, must also consider the risks and associated challenges of deploying these modern solutions in future ERPs. We provide a clarion call for practitioners to adapt, innovate, and deploy such advanced technologies into their ERP security frameworks. The aim of security and ERP research should be to develop, test, and deploy intelligent systems within our complex ERPs.

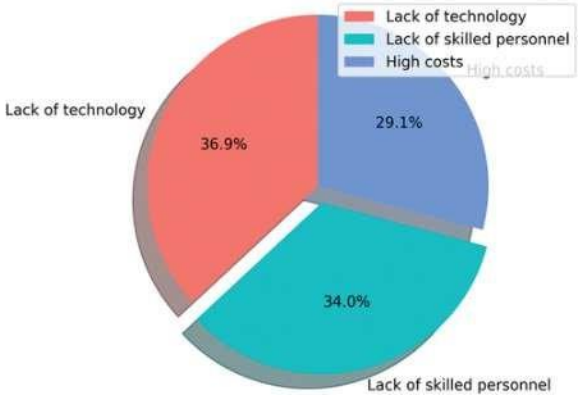

Fig : Current trends in AI and ML for cybersecurity

6.1. Emerging Trends in AI and ML for ERP Security

Recent years have observed a new interest in various AI and ML methods directly linked to ERP security to protect the huge amount of data and manage digital risk across the business world. The use of AI and ML provides digital risk analytics for identifying cloud-related threats and better management of cloud-based ERPs by automating various levels of the organization's activities. The integration of AI with blockchain, when used with business processes and relevant transaction databases, can provide long-

term data security across a wide organization. AI methods can offer new mechanisms to complete transactions based on continuous values by building erasable graph theory on transaction databases. There is a dynamic change in the views of management and scientists regarding the treatment of fraud, specifically for ERP security, with a completely new research direction, which includes securing faster Internet of Things transactions. Based on these pillars, there appears to be interest in IoT transactions for maintaining realistic physics of big data, thus creating a new research agenda resulting in this paper on fast-streamed Internet transactions. Methodologies include enhanced policies to detect anomalies in ERP systems and fraud through new sophisticated systems indicating unusual brain activities of IT infrastructures.

Emerging Trends Recent industry reports and research present various emerging trends in AI and ML to enhance ERP security, such as: - a greater and stronger association of AI/ML tools with ERP solutions by market leaders and vendors; - development of increasingly intelligent algorithms to address complex threat environments; - focus on more predictive capabilities; - increased use of sophisticated analytics to measure and monitor the effectiveness of security improvements; and - a shift in industry perceptions of the value of AI and ML tools, recognizing better alignment with real-world threats. A positive outcome of AI beyond increasing network security is improved network performance. However, two principal concerns about AI/ML tools drawn from these reports are the historic difficulty in fully utilizing the capabilities of these tools due to skill set limitations within user organizations, and for relatively larger international organizations, the almost ineffective state of AI/ML rigor against brand-oriented reputational attacks. It is also worth noting that there are parallel explanations for the relatively limited use of these tools. The effort to transition to new technology of this magnitude lies in incremental progression from the base starting point. Furthermore, human behavior is perceptibly influential in the appropriate adoption of the technology. In large part, as the Human Capitalist theory explains, an organization cannot deploy tools and systems it does not understand – either in technology, scope, or operational concept.

6.2. Future Trends

It is an open secret that technology is evolving at a rapid rate. Organizations need to think about better and effective security strategies to restore their existence. Looking at the security strategies, the incorporation of AI algorithms may grow in very high numbers dealing with various kinds of data, due to which cyber threats are increasing. The collaboration of AI technology and human beings in making decisions to make organizations more

secure and productive will gain importance in the coming years. Security strategies will adopt predictive analytics to uncover data theft techniques and patterns. It is also predicted that in future enterprises, AI algorithms will adopt real-time behavior-based monitoring of applications using big data tools and technologies for a proactive situation. The ethical considerations and changes that AI technologies can make will involve the security of privacy. On technological innovations, security should never be overlooked. Most researchers predict that AI technology will become more flexible and that in the future, AI technology will have proper use through preventive control actions. The model proposed involves various behaviors under different interactions of framed variables. For an exhaustive outcome on forecasts, interaction between many other variables will give way to the architectural model for future security.

7. References

[1] Syed, S. (2021). Financial Implications of Predictive Analytics in Vehicle Manufacturing: Insights for Budget Optimization and Resource Allocation. Journal Of Artificial Intelligence And Big Data, 1(1), 111-125.

[2] Nampally, R. C. R. (2021). Leveraging AI in Urban Traffic Management: Addressing Congestion and Traffic Flow with Intelligent Systems. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 86–99). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1151

[3] Vaka, D. K. “Artificial intelligence enabled Demand Sensing: Enhancing Supply Chain Responsiveness.

[4] Vankayalapati, R. K., & Syed, S. (2020). Green Cloud Computing: Strategies for Building Sustainable Data Center Ecosystems. Online Journal of Engineering Sciences, 1(1), 1229. Retrieved from https://www.scipublications.com/journal/index.php/ojes/article/view/1229

[5] Eswar Prasad Galla.et.al. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions Educational Administration: Theory and Practice, 27(4), 1228 –1236 Doi: 10.53555/kuey.v27i4.7592

[6] Syed, S., & Nampally, R. C. R. (2021). Empowering Users: The Role Of Ai In Enhancing Self-Service Bi For Data-Driven Decision Making. Educational Administration: Theory And Practice. Green Publication. Https://Doi. Org/10.53555/Kuey. V27i4, 8105.

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

[8] Mohit Surender Reddy, Manikanth Sarisa, Siddharth Konkimalla, Sanjay Ramdas Bauskar, Hemanth Kumar Gollangi, Eswar Prasad Galla, Shravan Kumar Rajaram, 2021. "Predicting Tomorrow's Ailments: How AI/ML Is Transforming Disease Forecasting", ESP Journal of Engineering & Technology Advancements, 1(2): 188-200.

[9] Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, Data-Driven Management: The Impact of Visualization Tools on Business Performance, International Journal of Management (IJM), 12(3), 2021, pp. 1290-1298. https://iaeme.com/Home/issue/IJM?Volume=12&Issue=3

[10] Syed, S., & Nampally, R. C. R. (2020). Data Lineage Strategies–A Modernized View. Educational Administration: Theory And Practice. Green Publication. Https://Doi. Org/10.53555/Kuey. V26i4, 8104.

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

[12] Gagan Kumar Patra, Chandrababu Kuraku, Siddharth Konkimalla, Venkata Nagesh Boddapati, Manikanth Sarisa, An Analysis and Prediction of Health Insurance Costs Using Machine Learning-Based Regressor Techniques, International Journal of Computer Engineering and Technology (IJCET) 12(3), 2021, pp. 102-113. https://iaeme.com/Home/issue/IJCET?Volume=12&Issue=3

[13] Syed, S. (2019). Roadmap For Enterprise Information Management: Strategies And Approaches In 2019. International Journal Of Engineering And Computer Science, 8(12), 24907-24917.

[14] Venkata Nagesh Boddapati, Eswar Prasad Galla, Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Gagan Kumar Patra, Chandrababu Kuraku, Chandrakanth Rao Madhavaram, 2021. "Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times", ESP Journal of Engineering & Technology Advancements, 1(2): 134-146.

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

[16] Kothapalli Sondinti, L. R., & Syed, S. (2021). The Impact of Instant Credit Card Issuance and Personalized Financial Solutions on Enhancing Customer Experience in the Digital Banking Era. Universal Journal of Finance and Economics, 1(1), 1223. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1223

[17] Vankayalapati, R. K., Edward, A., & Yasmeen, Z. (2021). Composable Infrastructure: Towards Dynamic Resource Allocation in Multi-Cloud Environments. Universal Journal of Computer Sciences and Communications, 1(1), 1222. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/1222

[18] Mandala, V., & Surabhi, S. N. R. D. Intelligent Systems for Vehicle Reliability and Safety: Exploring AI in Predictive Failure Analysis.

[19] Vankayalapati, R. K., & Rao Nampalli, R. C. (2019). Explainable Analytics in Multi-Cloud Environments: A Framework for Transparent Decision-Making. Journal of Artificial Intelligence and Big Data, 1(1), 1228. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1228