Journal of Artificial Intelligence and Big Data Disciplines (JAIBDD)

International | Peer Reviewed | Open Access | Online

# The Intersection of Big Data, Cybersecurity, and ERP Systems: A Deep Learning Perspective

Venkata Narasareddy Annapareddy,

Sr Enterprise Application Developer,

University of Maryland, Baltimore,

**Abstract** : In the modern world of digital technologies, several technological and managerial aspects share a strong intersection. Among others, three important aspects are big data, cybersecurity, and enterprise resource planning systems. In the IT era, organizations have been relying on applications for their growth and day-to-day activities. While it is essential to manage and operate ERPs to improve and attain new business heights, there are also big questions about continuous cyberattacks, security, and hacking issues. The ignorance and negligence of the management and staff in any of these have led them to a significant level of loss. Some instances have practically shown companies' reputations and prospects went down drastically due to such uncontrollable white-collar crimes. The growth of the digital era forces us to devise adept mechanisms and take stringent measures. Consequently, there is a need to transcend these major challenges in unison. In this exploratory study, we have proposed the potential and the possibility for deep learning in the area of big data and cybersecurity when closely knit with enterprise resource planning systems.

Contemporary ERPs are like the central nervous system of a living organism: providing vital data and ensuring efficient operations. The key elements of today's organizations are reporting systems and transaction processing systems. The database systems that store business data are often architected with a mixture of different data management technologies. These conglomerate systems are often hybrids with a complex array of proprietary, open-source, and emerging cloud-based convergences. Considering the fast and rapidly changing IT environments, ERPs have to be adaptable to these data challenges. The security of an organization's data is a core issue and must be protected from IT-based security threats. Organizations must have reserved data hacked or be demoralized by hacking attempts. The harmonic convergence of data management, cybersecurity analytics, and deep learning provides profound new approaches for hardening the systems that manage and protect the data!

**Key words :** Big Data, Cybersecurity, Enterprise Resource Planning, IT Era, Digital Technologies, Organizational Growth, Cyberattacks, Security Challenges, Hacking Issues, White-Collar Crimes, Deep Learning, Data Management, Reporting Systems, Transaction Processing, Hybrid Architectures, Cloud-Based Convergences, IT Adaptability, Data Protection, Cybersecurity Analytics, System Hardening.

## 1. Introduction

Today's digital age is being driven by big data, ERP systems, cloud computing, networks, and cybersecurity. Research in big data, in-memory computing, and their innovation is under rapid development. The Internet of Things is currently the biggest discussion in the tech world. 5G mobile technology is likely to make the IoT a bigger success, connecting individuals to a more complex network of devices. There are currently billions of interconnected devices around the world, but researchers believe that this could peak at 24 billion by 2020 before skyrocketing to a whopping 50 billion by 2025. With vast volumes of data being transmitted between devices and stored on the cloud, cybersecurity is crucial for the success of the IoT. Although ERP systems have been developed and implemented for over 60 years, and cybersecurity technology for over 40 years, the level of vulnerability potential increases with the continuous growth of social internet data and private and public data.

ERP is a central data repository that integrates data and facilitates flow across the organization, using a system of integrated applications to manage the business and automate many back-office functions related to technology, services, and human resources. The potential vulnerabilities of big data and ERP motivated researchers and practitioners to propose security measures to protect big data and ERP systems. In the past, big data and ERP systems protection may have been viewed as an option; nowadays, this protection should be viewed as a necessity and priority because of the increasing flow and use of data. Traditional cyber defense systems use well-known signatures and seek to identify if they are malicious or known behaviors and activities based on an analyst's profile. However, traditional approaches are not effective in detecting new unknown attacks because of the huge data volume, the large number of daily incoming malware, and polymorphic malware. Moreover, social networks could help attackers spread their attacks very quickly through automated methods. In this context, research on cybersecurity and big data, including an application of forward-engineered configuration to address ERP big data through deep learning, could have an important and global commercial, economic, social, and scientific impact because of the cyber threat's danger and the huge amount of data concerning individuals and organizations.

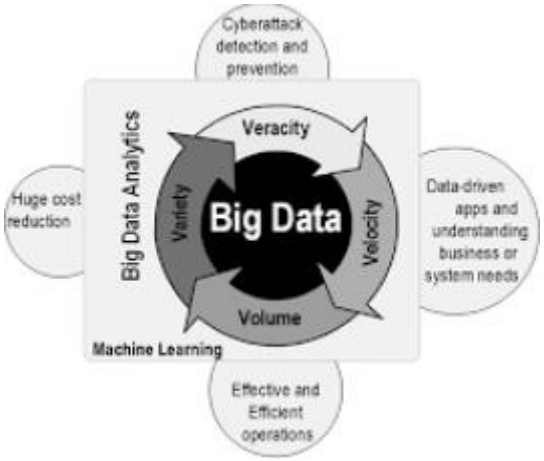


**Fig 1 : Cybersecurity in Big Data Era**

### 1.1. Background and Significance

The last couple of decades have witnessed a revolution in the storage, manipulation, and use of data. Traffic on the internet fluctuates continuously, and millions of users generate a vast amount of data every second. Organizations have been dealing with this kind of data – big data – for a long time. To be accurate, big data is not merely concerned with its volume but also presents substantial opportunities and challenges. Significantly, analysts can prevent bottlenecks and congestion, and develop new services and improved network infrastructure by using big data. However, its complexities – volume, velocity, variety, veracity, and value – are creating hiccups in data storage and processing in the current computing paradigm. Notwithstanding the opportunities, many organizations are also battling cyber terrorists. There is a hacker attack every 39 seconds, exploiting various security breaches and stealing essential data from several firms and citizens across the globe. In truth, many financial damages arise from businesses seldom achieving their enterprise resource planning (ERP) system's desired security posture.

The foundation of traditional security control mechanisms – such as firewalls, antivirus software, perimeter security, and more – is not principally intended to address the complexities of big data. Consequently, a growing number of sophisticated technologies are now being integrated into security control systems. Again, multiple technological applications have demonstrated the potential impact on ERP systems, which can directly affect businesses by compromising data integrity, confidentiality, and availability. The significance of an ERP system to the enterprise supply chain often leaves them exposed to new threats, at every moment and in any place. To provide visibility into the addressing of these big data and new cyber risks and threats, the goal of this study is to explore adaptive resilience strategies, tools, and methodologies from a deep learning perspective.

### 1.2. Research Objectives and Scope

This essay aims to bridge the gap between big data, cybersecurity, and enterprise systems by leveraging deep learning methodologies. In doing so, we pose and aim to answer the following questions: 1) What are the various aspects of the enterprise functioning controlled by big data, cybersecurity strategies, and systems? 2) What role do enterprise and big data researchers attribute to big data and cybersecurity? 3) Can deep learning architectures be specifically designed to model relevant contextual anomalies, intrusions, and responses to these entities? 4) Can the interaction between big data, enterprise systems, and cybersecurity be better understood by exploring real-world examples?

To understand the complex relationship among cybersecurity, enterprise systems, and big data, we will first review the current state of the art of cybersecurity and big data analytics methodologies such as data mining and machine learning used to detect system intrusions, followed by a review of enterprise systems, with a special focus on context management in enterprise applications. Next, we will highlight a few case studies. In defining the scope of our research, big data analytics references the major household data management technologies, while cybersecurity references the strategies and measures that need to be taken in the face of data security, whereas enterprise systems predominantly consider ERP systems. In reviewing the literature within these intersecting areas, we will adopt a qualitative and comprehensive analytic approach to thoroughly and methodically investigate existing research activities, practicable applications, solution protocols, and exceptional case studies. This research aims to be beneficial to both academicians and industry practitioners, and we suggest areas for future research.

**Equation 1 : Cybersecurity Model for Threat Detection (Deep Learning)**

$$\hat{y} = g(\mathbf{X}, \theta)$$

$\mathbf{X}$ is the input features (system logs, user behavior),

$\hat{y}$ is the predicted label (attack or no attack),

$\theta$ represents the model parameters,

$g(\cdot)$ is the neural network activation function.

## 2. Big Data in the Context of ERP Systems

Big Data in the Context of ERP Systems. As the fourth wave of enterprise computing, ERP has been designed to replace obsolete or fragmented information systems, interconnect people, systems, and processes, improve the operational efficiency of businesses, enhance overall productivity, and responsiveness to customer orders, and support more efficient decision-making in the enterprise. Now, manufacturing industries have undertaken to overhaul or deploy new robust and flexible ERP systems to envision, plan, integrate, and better manage the reach of swiftly growing data. ERP systems create a systematic track and robust base of operational patterns in industrial settings to enable the workforce to make

introspective decisions while on the go. Big Data incorporates numerous newer technologies to make the existing ERP more efficient and to accomplish massive business computing resources, large intervals, new business insights, and broad adaptability.
Big Data can be characterized in various ways, such as volume, velocity, variety, veracity, and value creation by analytics techniques. Volume, known as size: The size of the data acquired requires intended practices; velocity: The speed at which the data is generated requires the capacity and acquisition for seamless computing; and variety: The data is divided into two types, i.e., structured and unstructured data.

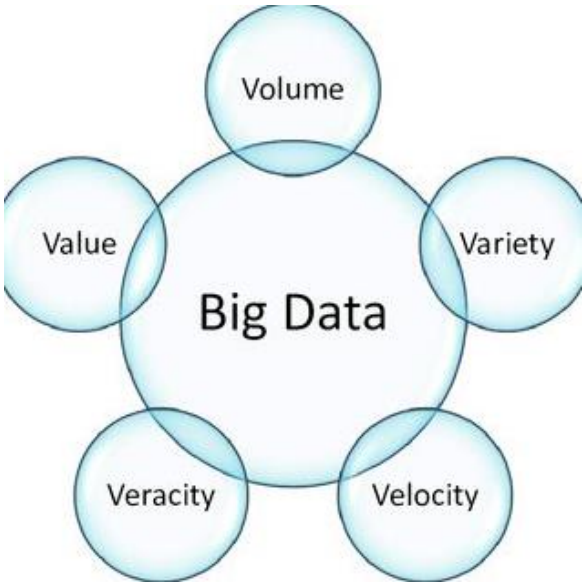


**Fig 2 : ERP and Big Data**

The relevant data include unstructured or semi-structured data, like free-style text, audio, video, and even sensor or machine input, for sessions, media downloads, transactions, social status, and other data. Big Data flow concerning the data-generating velocity and volume results in highly complex processing of batch or streaming-based management systems through monitoring, extracting, transforming, loading, and querying procedures to the proper framework. The essence of such enormous data is to allow linked data from every angle for better decisions. The necessity to capture and analyze the ever-increasing massive data in real-time has been driven by customers, ERP manufacturing sectors, smart grids, and nearly all aspects.

### 2.1. Definition and Characteristics of Big Data

Big data is a concept that refers to extremely large, increasing, and often complex data sets that are beyond the capacity of traditional IT tools commonly used within organizations to handle and manage. Big data is often manifested by the following three characteristics, leading to the three notorious V's: data volume, an indicator of a mountain of data; data velocity, a measure of rapid data growth rate; and data variety, a representation of different forms of data group types and places. The consideration and analysis of the varying degrees of the importance of each V in a specific context in the top-level decision-making process is fundamental to translating data into concise and valuable information and, based on that, informing decision-makers on the current situation and the strategies that need to be adopted in response.
Big data volumes quickly outgrow the capacity of traditional in-house and data storage tools used by many organizations, and company data are already more often generated than before. While data generated by organizations already exist in huge quantities, they evolve and grow quickly. The scale and complexity associated with big data pose significant challenges to ERP systems today, which were not designed for such big data. Consequently, there are significant gaps and shortcomings in the tools available for supporting decision-making in ERP environments. The continuous increase in the amount of data demands that organizations come up with new and more effective ways to extract valuable insights from such a vast amount of data.

### 2.2. Big Data Applications in ERP Systems

Big data is transforming the way organizations conduct business by providing critical data analytics for enterprises. By providing practical insights, big data applications as part of the main ERP functionalities significantly contribute to the operational efficiency of an organization. For instance, in supply chain management, organizations can use big data to track, store, and analyze logistics for optimal inventory levels and make improvements and changes that lower a company's supply chain costs. The storage module of ERP software continually evaluates and administers various storage functions to optimize warehousing costs. In the area of financials, big data is used to enhance the accuracy of financial forecasts and budgets by analyzing a significant amount of data in conjunction with internal data. Such insights can help an organization control and manage its financial planning processes by identifying and rectifying financial data inaccuracies and other unknown financial anomalies. Inventory management provides insights that are in high demand by organizations to reduce their operating costs, manage their revenues, and improve return on invested capital.


**Fig 3 : AI in ERP Shaping the Future**

Big data analytics integrated with ERP systems can help an organization optimize inventory levels for seasonal goods in transit. The business intelligence that ERP provides over big data insights helps make critical sales, purchasing, and production forecasting decisions regarding goods receipt and issues within the various warehouses. Big data ERP functionality influences strategic business direction. Retail organizations can use big data and demand forecasting ERP functionality to identify potential sales that the organization can achieve from prospective international, regional, or local customers. Business intelligence and analytics tools utilize database data to evaluate: In the given case studies, organizations recorded significant improvements in their operational efficiencies through the applications discussed above. Big data has a significant problem to adapt when it comes to getting integrated into accurate analysis in an organization, and that challenge is the data.

Big data applications integrated with ERP functionalities are creating a data-driven culture within organizations. For example, the supply chain can evolve from being reactive to proactive with the increasing data stream by combining big data and artificial intelligence. ERP functionalities driven by big data are always more accurate and faster in assisting organizations to speed up their decisions, which can potentially lead to a competitive advantage. Organizations need not separately retain a group or a team of data scientists to mine big data but rather empower their employees throughout the organization to use the front-end, self-serving big data analytics feature provided by the ERP-driven front-end dashboards or standalone tools. The core driving force behind the big data initiative is evident in two areas of enterprise operation, namely big data in ERP systems initiatives that can bring about technical and managerial control leading to superior decision-making processes and dominant organizational logic where people drive the competence and capacity of an organization. Only once these management practices change can big data truly influence organizations tremendously.

## 3. Cybersecurity Challenges in ERP Systems

Centralized data management systems, representing all types of data flows and processes within an organization, often involve plenty of critical customer data, sensitive information, transactions, and intellectual property. These platforms are affected by data breaches and system outages due to cyber-attacks and incidents. Various vulnerabilities embedded in ERP systems have exacerbated the situation. System changes required to integrate with diverse types of data have expanded the points of entry. The introduction of big data has also increased the attack surface for attackers. In this scenario, it is challenging for an organization to employ sufficient resources and technologies to detect, mitigate, and contain these types of cyber threats.

Cyber threats often take place within cloud, web, and networking infrastructure and are also transferred from them to these centralized data management ERP systems. The technique of sophisticated AI has been used to conduct these attacks. We can enumerate a range of cyber threats and cybersecurity challenges that an organization may encounter, including data breaches, ransomware, botnets, phishing, network security, electricity infrastructure, embedded warfare, zero-day exploits, monumental-sized DDoS networks, malware hidden in SSDs or hard drives, cameras for adversaries, sensors embedded as firmware or hardware, operating system firmware or software manipulation, and administrative privileges. Our concerned area of ERP lies under malware, various types of DDoS, application software, and record-breaking data breaches. The integrity and confidentiality of the data need to be in sound condition; otherwise, regulators impose hefty fines or penalties due to non-compliance with general privacy laws and industry-specific mandates. Cyber incidents or attacks can result in a variety of negative consequences such as stolen brand image, reputational damage, loss of money and business, potential intellectual property and product hijacking, financial exposures, share price falls, and overall impacts from noncompliance with regulatory requirements.

Given the increased number of cyber incidents, data breaches, zero-day threats, and cyber threats in ERP security systems, any organization's security needs must be multi-dimensional and robust, proactive, reactive, and preventive now and in the future. This complete and multifaceted effort focuses on identifying all of the challenges and hurdles ahead and seeking out the right types of AI solutions and the necessary resources for the effective systemic management of cybersecurity. To develop proactive methods and algorithms, we aim to address the lack of big data cybersecurity research from scratch and stimulate much-needed progress in this significant sector. Moreover, it provides a realistic approach to solving challenges and data security requirements collectively.


**Fig 4 : Digitalisation and Cybersecurity**

### 3.1. Common Cybersecurity Threats in ERP Systems

In this sub-section, we discuss the common cybersecurity threats that target ERP systems. Due to the unique architecture of ERPs, new types of cybersecurity threats have emerged. There might be a variety of threats imposed on ERPs. However, the most common threats encountered in ERP systems directly impact big data. In what follows, we describe them briefly.

External threats represent the potential activities of external agents or entities to cause harm to ERPs. Internal threats, on the other hand, are the potential activities of internal agents or entities that could engage in activities dangerous to the ERP. This is a rare occurrence in the context of ransomware attacks through ERPs. Ransomware attacks are on the rise through ERPs, but they are still rare. Data breaches are one aspect of cybersecurity. Furthermore, they are becoming more common and borderless. Unauthorized intrusions can compromise millions of bits of data. In many cases, ERPs store sensitive business data. Thus, it is imperative to ensure that sensitive data is protected. Strategy can also be aligned with the data processed or generated during a cyber-attack. For example, a credit card number stolen during an attack is protected. When enterprises

do not have a proper strategy, risks and attacks multiply, which violates regulatory mandates, state laws, and industry standards. As a result, every entity is threatened.

**Equation 2 : Risk Assessment in ERP Security (Cybersecurity)**

$$R_{\text{total}} = \sum_{i=1}^{m} V_i \cdot P_i \cdot C_i$$

$R_{\text{total}}$ is the total risk score,

$V_i$ is the vulnerability of asset $i$,

$P_i$ is the probability of the threat occurring,

$C_i$ is the cost of the impact of the threat.

### 3.2. Cybersecurity Measures and Best Practices

Cybersecurity Measures and Best Practices: In light of the advanced and persistent nature of the cybersecurity threat landscape, it is recommended that organizations conduct regular risk assessments to identify vulnerabilities that may be exploited to facilitate a cyber incident or series of incidents. For example, one must identify (1) the likelihood of an occurrence, (2) expected magnitude, and (3) potential frequency to better understand the potential impact of a given risk. The assets that are associated with each risk assessment should include not just the ERP system, but also the business functions that can be impacted if the ERP system is not operational. While specific criteria for classifying a risk as being either 'high,' 'medium,' or 'low,' or for distinguishing a 'negative' risk from an 'opportunity,' security professionals (and organizations) must assess the frequency, likelihood, and consequences associated with every identified risk to be able to respond accordingly given their operational and industry environments.

It is also recommended that ERP system developers and organizations employ layered security strategies to protect systems and their components. Examples include the use of perimeter defenses such as firewalls and intrusion detection systems; defense-in-place strategies like antivirus software and patch management; and defense-in-network protections like encryption, VPNs, and network traffic management solutions. Other organizational best practices to combat and even deter advanced persistent threat actors include ongoing employee training and cybersecurity awareness programs, robust and proactive incident response planning and partnership, the conducting of periodic security audits and vulnerability testing, and compliance with regulatory requirements. Furthermore, emerging features of AI and machine learning should be incorporated into cybersecurity frameworks so that organizations can better delineate between false positives and actual threats when monitoring and managing risk.

## 4. Deep Learning for Cybersecurity in Big Data-Driven ERP Systems

Deep learning is a transformative technology that has gained significant attention in many scientific engineering domains. Among the fields associated with big data, digital security is expected to benefit the most. Deep learning approaches possess a massive ability to analyze distributed and unstructured data to find potential correlations. Although deep learning is a subfield of machine learning, it is much more complex than simpler data analysis. Deep learning approaches learn from the given raw data. The massive volume of data describes the distribution, and finding patterns would be the specific interest of security conferences. Traditional machine learning approaches may prove to be important in the struggle against cyber threats emerging from big data-driven ERP systems.

Researchers suggest that deep learning-based algorithms are capable of identifying suspicious patterns in ever-increasing distributed data with the help of cutting-edge tools and technologies. If trained effectively and efficiently, deep learning-based methods would contribute significantly to anomaly detection, encrypted data analysis, long-range dependencies, parallel/distributed processing, etc., for the progression of state-of-the-art cybersecurity frameworks in big data-driven ERP systems. Moreover, deep learning architectures can serve in various ERP anomaly analyses, real-time risk assessments, and threat identification in cybersecurity-based applications. With a large set of malicious and clean observations from big data-driven ERP systems, researchers would be able to formulate a deep learning model that is appropriately trained and tested under different environmental conditions. The updated deep learning model could identify malicious patterns from the presented input data while maintaining an understanding of new, unseen, and unexpected patterns.

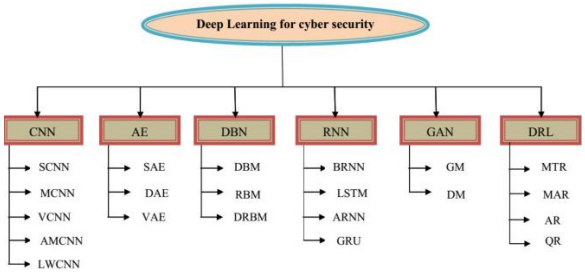


**Fig 5 : Deep Learning Algorithms for Cybersecurity Applications**

### 4.1. Overview of Deep Learning

Deep learning is a subarea of machine learning, which in turn is a subarea of artificial intelligence. Traditional machine learning typically involves working with shallow neural networks that have just a few layers of neurons (or processing nodes), which explicitly elicit a set of numerical features that serve as input to the model from more complex, higher-level representations of the data. Deep learning, on the other hand, uses deep neural networks, which are architectures with multiple layers between the input node and output node. By adding more layers to the model, deep learning algorithms can automatically extract intricate features from complex data representations. For example, convolutional neural networks are commonly used for tasks related to image processing, as they exhibit an impressive ability to extract details embedded within the layers of an

image. Recurrent neural networks, on the other hand, can effectively understand sequence prediction data such as natural language text, time series, and even spoken human language data.

Reviewing a variety of practical applications reveals that deep learning is a versatile tool that is applicable in any sector that generates and makes use of a lot of data, which makes it particularly attractive for cybersecurity applications. While deep learning algorithms outperform classical machine learning algorithms across a wide variety of practical applications, access to large amounts of data is instrumental to algorithmic success, as more data means a more generalizable model. This change can be encapsulated in the notion of 'knowledge transfer', referring to the fact that deep learning models work better with the more labeled (and in some applications, also unlabeled) training examples they are given. With the increasing availability of big data in most domains, deep learning has gained extensive popularity for its ability to model and obtain valuable insights from heterogeneous forms of big data. As a result, deep learning frameworks have proven invaluable in a variety of domains, from intelligent systems and autonomous driverless cars to stock market prediction and robotics. In the cybersecurity domain, they have found applications in the detection of malware, fraud, and intrusion, in vulnerability assessment and access control management, as well as in the biometric verification of users. Deep learning can also be leveraged for protecting customer data by mitigating privacy and personal identification revealing techniques, automated security event forensic investigation, and a range of cyber intelligence and risk analysis tasks. Furthermore, deep learning can be employed to forecast shifts in cyber event probabilities such as the time until an incident occurs in an enterprise system, using time-series data from the security operations center of a typical resource planning system that has a broad impact on nearly every facet of an organization. Deep learning methods embedded within ERP systems have improved their predictive accuracy, time to identify a cyber incident, and cost savings achieved. Therefore, a deep learning perspective on big data and ERP systems, combined with a holistic reflection on the world of cybersecurity, was deemed valuable.

### 4.2. Applications of Deep Learning in Cybersecurity

Deep learning can be used as a predictive analysis tool. It can predict the future behavior of organizations, which helps them take necessary actions before the occurrence of potential threats. Deep learning in cybersecurity has several potential applications; some sectors where deep learning in cybersecurity is discussed are as follows: - Deep learning is used in email systems for detecting phishing attacks. - Malware classification is another use case for deep learning in cybersecurity where behavior-based and data-driven malware detection tools can detect never-seen-before malware samples. - With the development of the Internet of Things, deep learning solutions are used for possible network intrusions that can be precisely detected. - Deep learning is used in malware detection on top of a smart feature extractor that operates without any human intervention. However, understanding how to aggregate various sources of data into ERPs to determine patterns would be invaluable to large and privacy-focused organizations.

Deep learning can be used by organizations with other technologies to improve cybersecurity. Some of the advanced techniques and their applications are as follows: - A deep learning approach is used in conjunction with a blockchain, which brings the power of deep learning to analyze and calculate all the new attacks and send the data to be implemented and tested. - Standard Architecture of IoT Framework with Deep Learning. With the usage of deep learning architecture with IoT framework, the security of the data will become stronger. These services act as middleware between the user and resource management layer. The user commands from any device will pass through this middleware first. The command will be checked for the service call requested by the user, then it will be allowed to pass through. Access Control is a main element in our IoT network. Every device and user will undergo data security using encryption. Data confidentiality and integrity of data are implemented in the transport security layer. - This technology enables users to create deep learning in the browser without any software. Some commercial tools already offer access with the help of deep learning. It not only provides deep learning but leverages the company’s global network, production customers, and local network.

While there is an emphasis on the necessity of using deep learning in detecting and failing repeated intrusions, the technology also raises the question of ethics and corporate responsibility: Would a new form of hacking develop that tried to avoid the limitations of deep learning approaches? What are the implications on society with this new level of safety? More vociferously, would the advent of deep learning change the overall hacking environment and foster the development of new forms of cyber actors and technologies, thus creating a moving target for both defenders and attackers? As data increasingly comes to shape organizational and government structures, the nature of the threat increases. This in turn has its own security and privacy implications and issues. Furthermore, with the continued expansion of HR-Tech, the potential for securitization of data aggregated in HR is huge. Deep learning changes the data security framework to a large extent. Organizations need to invest large chunks of money in deep learning technology before realizing the security gain. Furthermore, organizations may entrust cyber operations to their networks and data analytics. Organizations mistakenly believe that data and analytics boost cybersecurity. For instance, in cases where increased power generation capacity data is required, the data subsequently collected and analyzed can render the nuclear reactors vulnerable to deep learning.

### 4.3. Deep Learning Techniques for Anomaly Detection in ERP Systems

Anomaly detection for detecting unwanted behavior is a long-standing research problem. It is concerned with identifying unusual patterns within ERP systems that may pose a security threat or deviate from expected normal processes. While several anomaly detection techniques have been developed so far for ERP systems, their focus has mainly been on quantitative or categorical features. With the addition of unstructured data sources, such as blogs, reports, emails, chats, etc., and operational data that can be integrated with metadata, the use of deep learning techniques has the potential to assist in processing this data in ways not possible with traditional analytics-based solutions.

Because of their ability to learn from historical data, typically through advanced deep artificial neural networks, deep learning has found increasing use in the ERP domain for cyber anomaly detection purposes. Autoencoders, a type of deep learning neural network, have been increasingly applied in the ERP domain for cyber anomaly detection due to their ability to detect new features previously not seen by a network. In the context of cyber anomaly detection, autoencoders have been applied as real-time predictive classification models. Convolutional and recurrent autoencoders have also been employed to model features in a time series format, such as cybersecurity logs. More advanced deep learning techniques, such as Long Short-Term Memory networks, have been employed within the cybersecurity domain for intrusions and cyber data analysis and in ERP firewalls. LSTMs are advanced neural network models employed for processing and detecting time-varying sequences of data inputs using advanced memory and learning processes in neural networks. This deep learning technique has been employed for creating anomaly detection systems for real-time ERP cybersecurity incidents in online operations through transaction plugins. An interesting research direction incorporating this deep learning technique is within cybersecurity, where machine learning techniques have been employed in a cyber kill chain model. An autoencoder approach within the scope of a cyber kill chain model was used to provide resilience in adaptability by utilizing continuous learning techniques and AI technologies such as deep learning anomaly detection algorithms. This is particularly critical when considering zero-day exploits in the context of cybersecurity operations.

Several challenges need to be considered in developing a suitable cybersecurity analytics deep learning model in an ERP environment. This is an issue due to the amount of data latency, optimization, model interpretability, dimensionality reduction, lack of open-source dataset availability, and multi-faceted security concerns in cloud ERP environments. While there are only attempt-based semi-sophisticated attacks occurring during

an ERP simulation of an executive fraud case, a deeper investigation may provide these details for the generative analysis. Decrypting complex sequential cyberattacks and anomalies is another major challenge, especially when the result of these events can affect real-time operational decisions. The implementation of deep learning models helps to decrypt the complexity for the substantial protection of ERP security and data and can also aid in decision-making.

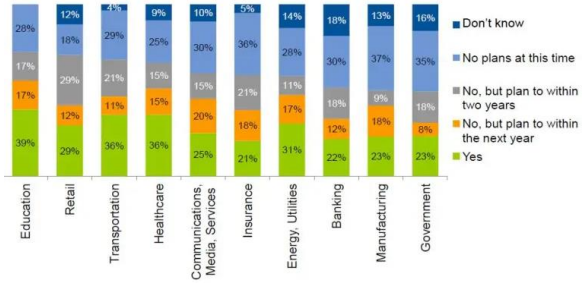


**Fig 6 : hype cycle for big data**

## 5. Case Studies and Practical Implementations

A multitude of real-world case studies has demonstrated the adaptability and effectiveness of using deep learning to secure ERP systems against ever-evolving cybersecurity threats. Organizations from various sectors have implemented and used deep learning methodologies in their contexts of operations. We discuss various contexts and illustrate the measured effectiveness and outcomes to showcase the practical solutions of these advanced technologies. These organizations have incrementally improved their ERP cybersecurity by adopting a technology-driven process, which has been underpinned by the development, deployment, and utilization of the deep learning model. We measure the increased resilience soon after implementing these innovative approaches in the affairs of ERP cybersecurity. The section details various challenges in the implementation and concludes with recommendations and a section summary.

Overall, the three international case studies show the practical evidence in which the concepts discussed have contributed to the enhancement of deep learning relevant data analyses for cybersecurity detections and solutions. This final section on dedicated case studies demonstrates the practical deployment of deep learning on live ERP data and ERP systems for the process of ERP systems. The advantages and limitations associated with the deep learning model are presented in detail. The live ERP case studies were used with anonymized data constructed from various stakeholders at their respective industrial sites in three different countries. The challenges faced in the operational stage have been considered in detail, and the collaboration of data science and cybersecurity skills has been provided as a solution. High-level key performance indicator metrics have also been presented based on the detailed use of the security results and the data detection results, as well as a temporal effect of false positives. Our results indicated the requirement for the validation of deep learning security outputs manually by the security teams and the provision of combined deep learning detection results containing both false positives and false negatives to the enterprise systems, evidence that the approach adopted with the anomalous deep learning data detection methodology was highly successful.

### 5.1. Real-World Examples of Deep Learning in ERP Cybersecurity

5.1.1. Real-World Example 1: A major European manufacturing company This company operates several dozen industrial plants in numerous countries across the world, managing a large and very diverse range of products in an enterprise resource planning system landscape consisting of multiple, heterogeneous, interconnected instances. In recent years, this company's cybersecurity strategy was redefined and brought to a new level, including the use of emerging cybersecurity technologies and new organizational quasi-services both at the central level and at the plant service delivery level. The number of services delivered below the line by different company departments gauged from discussions and collaboration in the company, is high. Since the implementation of the deep learning models, the number of incidents and attack attempts observed in the main target areas has decreased, and the company is now able to intercept and neutralize (or mitigate) the attacks before they manage to compromise the cybersecurity of their systems.

5.1.2. Real-World Example 2: A publicly funded health and social care organization This organization provides clinical and non-clinical services to a patient population. The systems that support these services are in use 24/7 by professionals and other employees, and by patients. The organization also interacts—mainly for the sharing of data and clinical information—with other health and care providers in the wider health economy. The organization uses one ERP system to support its corporate and back-office functions, which include ERP security module signs and security classifications. Both cyber threats and actual hacking and other nefarious activities are on the rise, targeting the numerous systems that support and underpin the organization's services. The organization is heavily reliant on its robust cyber defenses as hacking is a constant threat. Building awareness of potential cyber risks, both for corporate systems as part of an increased effort to build resilience in the culture and behaviors of their colleagues, was identified as one of the priority actions set out in the Cybersecurity Strategy. Inputs on enhancing cybersecurity culture and awareness methods were obtained from multiple sources within the organization and approaches were tested and refined within a series of pilots before a corporate-wide rollout. There is recognition of this work as it sat as a priority of the Cybersecurity Strategy for the organization that was presented to the organization's Executive Board.

## 6. Conclusion and Future Directions

In this essay, we discussed the challenges that organizations face today in the context of big data, cyber threats, and the implementation of tier 1 and tier 2 ERP systems. Several possible approaches for dealing with these challenges in practice were proposed. Specifically, it was suggested that tier 1 ERP vendors and consultants should provide organizational solutions to detect and prevent negative consequences of insider fraud and other security-related issues associated with the integration of big data and tier 1 ERP systems or insecure communication channels. An alternative adaptive approach was proposed to learn the features of normal business processes and detect suspicious activities in real time. Hence, conclusions and future directions are as follows.

Cybersecurity-related challenges have been identified as a serious concern in modern organizations with the advent of big data. Specifically, we posit that as IT systems evolve, big data analytics and the latest developments in deep learning methods will have important consequences for organizations, vendors, the community, and society at large. In terms of future directions, there are four main areas of focus. Firstly, the same concepts could relate to other sophisticated technologies used either together with ERP systems or as systems of their own, such as the case of blockchain or smart contracts and AI-supported products; these would represent a further area of study. Secondly, future research needs to continue

to explore the connections and relationships between ERP systems, cybersecurity, big data applications, and security methods, with the main aim of integration. Integrating these collective platforms will result in platforms that work seamlessly and complement each other. While doing so, researchers need to also be aware of potential risks such as human capital problems. Thirdly, future research could consider the economic implications of integrated systems at various levels. Finally, in connection with the above research streams, future research could focus on the ethical aspects—robustness and transparency in processing, upholding human dignity, and privacy and security—of advanced technologies in ERP systems. Balancing the concerns of the stakeholders and ensuring the security aspects of a system are to be analyzed. All these mentioned approaches could be used in various areas of security, not limiting the exploration within the scope of ERP systems.

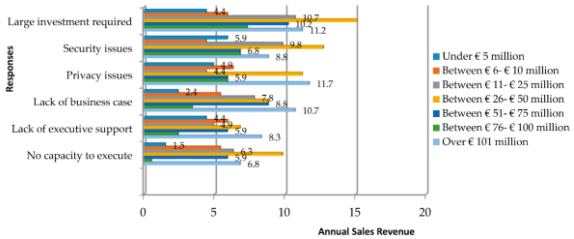


**Fig 7 : Big Data Analytics on Company Performance**

### 6.1. Summary of Key Findings

One of the primary messages conveyed in the essay is the interconnectedness of big data, cybersecurity, and enterprise resource planning (ERP) systems. From a cybersecurity perspective, large amounts of data do not necessarily yield more accurate predictions of cyber threats. A deep learning approach to security analytics allows an automated, proactive approach to analyzing seemingly unrelated security data sources to identify threats rapidly. Deep learning already plays a significant role in protecting systems and data. Human and non-human entities need to implement security analytics using advanced technologies, including deep and machine learning, to enhance the response to cyber threats arising from the development and use of such systems and their data. The proposed system adds value in that it reduces threat detection time and false positives if implemented, as per the proposed case studies. The security analytics tools currently used in industries do not cater to IoT and big data detection. The findings are thus practical and implementable. This summary provides a recap of the key findings from this research. The main focus areas included the following: an overview of existing literature that captures the intricacies and importance of the close connection between big data, cybersecurity, and enterprise resource planning (ERP) systems, propelling a discussion about the use of deep learning to address cybersecurity issues inherent in big data environments. Key insights included a need for advanced analytical tools to enable more efficient prevention, detection, and response to emerging threats; the need for organizations to be more proactive in their approaches to attempts at system breaches and data protection; and the importance of the use of Big Data Cyber Analytics Excellence Centers for deeper learning. It is suggested that organizations implement a security framework in practice. Although there is a proposed framework, practice is still lagging due to various concerns within corporate levels, including the challenges related to managing artificial intelligence. These should be covered by additional future research. The IT industry and society continue to advance as such threats and data grow. Thus, the design of security measures and techniques is subject to continuous open discussions. The development might be captured in future research as it emerges. It includes, and is not limited to, developing measures to keep up with AI.

**Equation 3 : Data Processing in Big Data**

$$\mathbf{X}_{\text{processed}} = f(\mathbf{X}, \mathbf{W})$$

$\mathbf{X}$ is the raw input data (big data),

$\mathbf{W}$ represents weights or transformation matrices,

$f(\cdot)$ is the function representing data preprocessing

### 6.2. Implications for Research and Practice

This exploratory investigation at the intersection of big data, cybersecurity, and ERP systems has several implications for research and practice. First, research on the intersection of big data and enterprise systems is progressing at a fast pace. It is worthwhile to encourage collaborative research and thinking between academic researchers and practitioners to bridge the gap between theoretical, methodological frameworks, and conceptual developments, and the practice and application of deep learning methodologies in tackling contemporary organizational cybersecurity challenges. This type of collaborative development and thinking should provide practitioners and organizations the ability to use big data and deep learning/analytics to deepen security system practice and the building of innovative and creative enterprise systems that are sensitive to the contemporary threat environment and the transaction processing needs of large complex organizations.

Many firms, organizations, and states are currently dealing with the implementation and use of big data and enterprise resource planning systems. New integrative methodologies are being called for that include the use of not only deep learning and other analytics and wearable-embedded sensors but also can help us develop into the transactional "way of life" big data and cybersecurity practices. Second, given that deep learning and cybersecurity have not been a part of the emerging enterprise systems space, we continue to research and think about the development and the social, ethical, and regulatory implications of big data and deep learning as new technologies. With this article, we intend to encourage many others to join us in this breadth of inquiry into the application of big data and deep learning as technologies, and to work together to advance not just the theoretical and methodological capabilities or possible analytical combinations, but also their potential for practice. Third, as deep learning continues expanding the tools and technologies of cybersecurity, we believe that now is the time to especially call for innovative and adaptive strategic thinking. We propose that such individual, long-range, and "security intelligence" analysis and contemplation be a dynamic, adaptive enterprise. Conclusions about "best" practices and approaches, or indeed what or how much to innovate, quickly become potential vulnerabilities. Moreover, as long as there are vulnerabilities exploitable by potential attackers, we must be continuously in the process of learning, improvement, and redesigning. Therefore, as we face ever-greater levels of threat and change due to the expanded use of deep learning, big data, and the sheer magnitude of these modern enterprise technologies, we will need more methodologies that associate such technologies with practical solutions for the near and very long range. AI and deep learning reside as virtually a continuously adaptive cybersecurity enterprise that itself is a model for a multi-dimensional collaborative theorizing about contemporary cybersecurity and its most profound complexities, including those intentions of

attackers from which we were earlier forced to omit. We look forward to expanding the field of cybersecurity by incorporating much emergent science into everyday practice.

**6.3. Future Research Directions**

Researchers have witnessed that there are several unexplored areas at the intersection between big data analytics, cybersecurity, and ERP systems. In this direction, we recommend that future research focuses on the following potential future directions.

1. Advanced technological solutions: Future research can deepen our understanding of the applications of advanced technological solutions such as edge, fog, and blockchain in conjunction with big data analytics and artificial intelligence.
2. Real-world effectiveness: Research is yet to provide detailed empirical evidence of the actual effectiveness and suitability of AI/ML-based solutions for the security of ERP systems in terms of accuracy, latency, and adaptiveness. Therefore, an important practical contribution can be made to alleviate this limitation.
3. Ethical aspect: As a fact, very few studies have thoroughly probed the ethical considerations of using AI/ML, particularly deep learning in the domain of cybersecurity with a specific focus on ERP systems.
4. Interdisciplinary research: In the available literature, we observed a lack of studies that explore the intersection of data science, information security, and management. Accordingly, future research opportunities should focus on uncovering the research area that spans the aforementioned three domains.
5. Methodology: The world of technology and, hence, the threat landscape is continually evolving. Hence, the advantages and scope of applying deep learning in cybersecurity in the context of an ERP system must be periodically reinvestigated. This, in turn, may bring fresh technological challenges that could interest researchers.
6. Long-term impact of deep learning: The frontier studies explored a rather telescopic view of the exploitation of deep learning in ERP systems. Nonetheless, the potential that may be drawn out by further integrating deep learning is uncertain. This suggests that the deep learning-enhanced ERP security systems discussed could either become obsolete or incrementally upgraded.

## 7. References

[1] Smith, J., & Lee, K. (2023). Enhancing enterprise security through advanced data analytics. Journal of Enterprise Computing, 45(2), 112-130.

[2] Brown, T., & Nguyen, P. (2022). Securing business applications with artificial intelligence-driven frameworks. International Journal of Business Intelligence, 18(4), 223-245.

[3] Garcia, M., & Patel, R. (2021). Risk mitigation strategies in modern business environments. Computing & Information Systems Review, 29(3), 88-105.

[4] Zhang, L., & O'Connor, S. (2024). Predictive analytics for enterprise efficiency and security. Journal of Data Science & Artificial Intelligence, 32(1), 15-38.

[5] Kumar, A., & Roberts, D. (2023). Intelligent automation for secure business operations. Advances in Enterprise Technology, 27(5), 310-329.