Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

AI-Powered Big Data and ERP Systems for Autonomous Detection of Cybersecurity Vulnerabilities

Srinivasa Rao Maka, Krishna Madhav Jha, Purna Chandra Rao Chinta, Chethan Sriharsha Moore, Niharika Katnapally, Gangadhar Sadaram

[1]North Star Group Inc, Software Engineer
[2]Topbuild Corp, Sr Business Analyst
[3]Microsoft, Support Escalation Engineer
[4]Microsoft, Support Escalation Engineer
5Amazon, BI Developer
[6]Bank of America, VP DevOps/ OpenShift Admin Engineer

This essay discusses the importance of AI-powered big data and ERP systems for the autonomous discovery and detection of cybersecurity vulnerabilities, for securing information from cyberattacks, and for preventing security breaches. Given that privacy is the fundamental principle for data-driven businesses, the rising relevance and effectiveness of advanced technologies become critical. The proposed concept explains the need for the mentioned technologies and the principles and mechanisms of their integration. This discussion is followed by an analysis of the direct implications of these concepts on regulatory requirements. The outcome of the project can be used to provide deep insights into the industry, define research directions for the near future, and guide further technological developments. The relevance of AI, big data, and ERP systems represents essential technological assets for enhancing cybersecurity solutions to ensure advanced protection from data breaches. On the other hand, AI-powered techniques also represent strong instruments for threat actors, valuable tools for creating zero-day attacks. This paper discusses AI-powered big data solutions and ERP systems as enablers for the autonomous discovery and identification of cybersecurity vulnerabilities. The way they are integrated and the results in terms of efficiency represent the core topics. The first part of the research presents the identified need for AI-powered big data and ERP systems and their incorporation as a key asset. Their underlying principles and mechanisms to create a highly secure environment with additional protection and privacy in today's ever-changing, complex, and digitalization-driven industries are suggested. The concept presents the implications in terms of regulatory requirements. The concept's proposed goal of convergence between AI-powered big data and ERP systems defines the last section of the project.

Keywords: AI-Powered Big Data, ERP Systems, Cybersecurity Vulnerabilities, Autonomous Discovery, Detection Mechanisms, Cyberattacks Prevention, Security Breaches, Privacy Principles, Data-Driven Businesses, Advanced Technologies, Integration Mechanisms, Regulatory Implications, Industry Insights, Research Directions, Technological Developments, Threat Actors, Zero-Day Attacks, Protection Mechanisms, Digitalization, Secure Environment.

1. Introduction

Nowadays, new legislation is often proposed and prioritized as a response to increased concerns regarding the state of cybersecurity. It is an unfortunate consequence of actively increasing our reliance on technology. The most effective way to gain control of something is to instantly shut it down, which makes compromised national infrastructure and security threats all too easy for attackers who obtain unauthorized access to it. Modern efforts to increase the security of these systems have so far delivered less-than-perfect results. When we are reactive, such as updating blacklist databases of commonly used threats, it is clear that our problem is not on time or ahead of the curve. With the accelerated development of continuously learning big data analytics and AI, we must now explore how to enhance both the mechanics and timing of our system's response.

There is already an established precedent for utilizing AI technology in response to concerns surrounding data security. Network traffic is one of the most comprehensive types of data that an information security team will be able to acquire; it is better to avoid interpreting proprietary data when first studying AI and security. Large businesses have always been reliant on data and information to drive strategic decisions and optimize operational efficiency. One of the ways many large businesses achieved recognition and success was with their Enterprise Resource Planning systems. Nowadays, businesses also have a focus on security, believing that secure systems are a corporate responsibility. Large businesses have increasingly massive datasets, known as big data, due to the ever-growing number of connected devices and the drop in storage costs in recent years. This text looks at the possibility of utilizing the informative aspects of big data that are typically ignored in the administrative use of ERPs, focusing on AI to develop APIs that let software learn to autonomously replicate ERP processes. These processes would need to precede financial access; not only to ensure a minimal increase in risk when integrating new credit systems with ERP, but also to further the reduction in people who have the highest access to these systems.

1.1. Background and Significance

Cybersecurity issues are increasing day by day, and an enormous amount of personal, company, and state secrets are being exposed to the world. Current network systems cannot detect and prevent emerging unknown threats before they achieve their goals of victimization. Most captured executable malware escapes detection from antivirus scanning due to the plethora of packed executables and encrypted propagation mechanisms in the networking environment. Most research on malicious activity has focused on the detection of intrusion attempts. Some of this work assumes that the attack or intrusion data is independent and identically distributed. The more modern networks are based on technologies such as advancements in AI and big data technologies. Such current systems aim to collect data on new vulnerabilities, analyze them, interpret the data, and then generate alerts or provide preventive measures to curb the effect of emerging cybersecurity vulnerabilities by predicting different risk factors associated with them.

Cybercrimes are becoming more sophisticated, such as ransomware and data breaches. The average cost of sensitive data breaches for enterprises was estimated to be between $100,000 and $4.6 million. Further, it was reported that more than 77,000 cyber incidents were reported in a given year, showing a 10 percent increase over five years that resulted in an estimated $20

billion of direct losses. The average total cost of a data breach was $3.62 million, with the average cost for each lost or stolen record containing sensitive and confidential information being $141. Many researchers suggest that war in the next generation will include cyberwars constrained to cyberspace or global networks. The statistics show that there is a need to find new mechanisms to detect vulnerabilities in systems for the security of stakeholders throughout the globe. Some of the previous studies did not address the integrated risk management solution that integrates AI, ERPs, and big data.

$$V_s = \sum_{i=1}^{n} \alpha_i \cdot g_i(X, Y)$$

Equation 1 : Vulnerability Detection Scoring Model

Where

V_s: Vulnerability score

α_i: Weight assigned to the i-th feature or pattern

$g_i(X, Y)$: Feature function analyzing big data X and ERP activity Y

n: Total number of features

1.2. Research Objectives and Scope

This research aims to address the following questions: Will the development of authentic infrastructure for the autonomous detection of cybersecurity vulnerabilities assist in improving organizational systems? What is the impact of AI-powered big data on autonomous ERP risk and impact management? In what way are advanced ERP systems linked to cybersecurity risk management? The research objectives and the scope are reflected in the questions being asked. The research will not focus on theoretical aspects of AI, big data, and new-era ERP. However, actual operational approaches will go hand in hand with cybersecurity protection approaches, controls, management, and reporting. Relevant choices and extensive use of the new knowledge will reduce the scope of thought on those associated measures within particular organizations. This research will commence with the examination of the effectiveness of AI-powered big data in detecting vulnerabilities. However, AI research aligned with cybersecurity aspects and data science has been reported. This research adds distinctive value to the existing AI and big data in terms of cybersecurity vulnerability perspective. Furthermore, the particular research is ERP-related potential incidents, with particular relevance for senior managers in control of core ERP/IS operations that are a key concern these days. The chief purpose of this piece is to double-check if and where artificial intelligence and big data can correlate, boost operations, and provide a protocol to improve this further - the secure ERP. Further scope will inspect the extent to which the most exhaustive, leading-edge ERP platforms have been scanned for the high severity and intensity of all vulnerabilities found.

Fig 1 : AI in Cybersecurity

2. Understanding Cybersecurity Vulnerabilities

The digital transformation has brought numerous benefits to organizations; however, this shift exposed different types of vulnerabilities that can have different impacts. Technical vulnerabilities, such as misconfigurations, unsupported operating systems, and inadequate security components, lead to the cause of many data breaches these days. Furthermore, procedural and personnel vulnerabilities can enable threat actors to bypass cybersecurity defense mechanisms to obtain unauthorized access to systems. People, processes, and machines play a vital role in the activity of collecting, processing, and storing data. Global surveys show that reports related to privacy and data protection issues, data breaches, security incidents, or recently discovered security vulnerabilities contribute to a substantial decrease in the reliability of organizations offering goods and services online, especially when personal information processing is involved. As the threat landscape continues to evolve, it is critically important to understand the types of vulnerabilities that exist as a first step for developing a sustainable cybersecurity capability.

In traditional security operations, security information and event management platforms passively observe and monitor the organizations' systems. Furthermore, application performance monitoring and network performance monitoring focus on operations. These monitoring systems detect alerts from sensors deployed across the enterprise when a signature or anomaly is detected. Particularly, these detection ratios find alerts on less than 50%, emphasizing their lack of best performance. Security information and event management platforms have log sources for cross-reference and can produce security incidents; these sources can be used to determine the malicious activities that occurred on the network. However, a security information and event management system uses signature and rule-based detection methodologies, so it has a hard time in real-time analysis as well as real-time responses.

2.1. Types of Cybersecurity Vulnerabilities

In the digital world, vulnerabilities are errors or misconfigurations within information systems and networks, which make them potential attack targets where the confidentiality, integrity, and availability of data and systems could be violated. Based on their nature, from different perspectives, cybersecurity vulnerabilities can be categorized into the following.

2.1.1. Technical Flaws

Technical flaws represent the prevailing stream of vulnerabilities causing the majority of

incidents. The essence of internal components, devices, protocols, and mathematics composes this class. The cleartext internet services, which disclose and collect personal data and place all transactions on untrusted internet applications, represent a pool of weaknesses whose abuse can cost verifiable losses. Collaborative research has elaborated these vulnerabilities in diverse application domains.

2.1.2. Configuration Errors

Configuration errors represent a subtype of technical flaws and involve the use of deployment and design defects by malicious attackers. Security in these settings demands more than just supply chain standards and laws but must consider humans for the assurance of cybersecurity and privacy. Incidents affected by configuration errors in smart building systems, including sabotaging patient treatment plans and replay attacks with stolen IoT devices, where the failure of application-level security can be directly traced to device misconfiguration or latent hardware vulnerabilities, were reported and demonstrated, respectively. The configuration of the outside threat scenario can be a mixture of technical flaws and characteristics of the software and hardware devices and settings.

Fig 2 : Vulnerability in Cyber Security

2.2. Challenges in Traditional Detection Methods

Several limitations are observed with existing cybersecurity detection approaches. Traditional methods are commonly based on signature-based detection, which limits the ability of security administrators to detect an emerging attack or vulnerability within their enterprise network. Actual detection and response occur after a delay post-attack, as a result of low defense-in-depth support, limited personnel, and manual processes. The detection speed can be further slowed down by the rapid growth in data volume and variety that security systems are required to handle. Moreover, the detection-response efficacy is compromised by the increasing complexity of the various field protocols and packet regularities. The large data volumes in transit can provide opportunities for covert channel communication and steganographic operations, which remain unresolved. Finally, cyber threats evolve to present new types of attacks that frequently utilize new types of exploits and vulnerabilities. Thus, zero-day attacks can lead to devastating results. Without new and advanced strategies for identifying vulnerabilities, the weaknesses, regardless of sophistication, within these ERP systems will continue to be exploited.

In response to these drawbacks associated with the existing cybersecurity detection methods,

there is an urgent need to develop a more automated, dynamic, and proactive system that can rapidly and efficiently identify emerging vulnerabilities. These systems that can collect, analyze, and respond to data in real time can instantaneously detect and respond to ongoing attacks. To reduce the burden on security staff, detection, and response must employ a learning or confounding component that is adaptive, thus responding to the actual threats, subsequently reducing false positive reports. The use of artificial intelligence can also lead to more accurate and in-depth detection while curtailing the associated human oversight errors. Crucially, new capabilities must be developed to rapidly search through, evaluate, and utilize the large amounts of data used for detection. This would allow for a more rapid flow of feedback consequent to detection, thus allowing for more timely and accurate response strategies.

3. AI and Big Data in Cybersecurity

AI is the science of training machines to copy human-like cognitive functions traditionally executed by humans, which includes learning, understanding, reasoning, problem-solving, and self-correction. One of the main goals of AI is to enable machines to predict the outcome of specific events, situations, or actions with increasing accuracy, to be able to aid in decision-making processes. Big data typically refers to a volume of data that has a size in the range of petabytes and exabytes, often stored in large distributed and parallel storage systems. From the term "big data," typically the following three "V" parameters are used productively to describe: (i) volume—defines the capacity or size of the data; (ii) velocity—defines the speed at which data flows from both sensors, mobile devices, social media, clickstreams, machines, and data from different applications; and (iii) variety—defines the different types of data that are sometimes used to describe information stored in numeric data, texts, images, or video formats.

AI technology complements big data systems to extend the ability of the processor to help recognize the pattern of data occurrence, make decisions and predictions, and provide solutions at the data center level systems such as intrusion detection, reporting of improper behavior, and capturing the abnormalities and their origin that happened before any hacking attempts manifest. AI can make predictions and determinations through applications to diagnose the possibilities of intrusion attacks into the system and also to demonstrate prevention systems based on network firewalls. AI and big data are gradually attracting attention to the advancing capabilities in their combinations of imposing advanced organizations within the field of information security. AI employs real-time analytics and logging to monitor for patterns and allows for predictive analytics, i.e., to discover patterns—maybe from a combination of data sources. When implemented in the form of machine learning, AI facilitates decision-making in terms of recognizing secure connections and warning administrators of anomalies. Big data can help unveil relationships between various asset groups and IDs. It also helps profile and identify risky groups and detect abnormal client activities. Emerging AI and big data technologies point toward the potential to prevent events from even penetrating a system. The use of big data to store, analyze, perforate logs, and monitor files appears to be superior since the technology processes tremendous amounts of incoming data and not only stores it but uses the information to identify compromised data and also compares it against other entities.

Several case studies deliver evidence that the integration of AI and big data has produced successful outputs in various cybersecurity protocols, such as monitoring and detecting security incidents, vulnerability assessment improvement, and detecting abnormal behavior. AI combined with cyber data is very effective in identifying security vulnerabilities. This combination helps organizations gain insight into their assets, detect if these nodes have relevant active services if the operating system and credit card processing are valid, and if public exploits or malicious traffic can affect vulnerabilities. This works in combination and with permission from administrators to deploy agents on the assets examined. AI is also seen to be integrated with big data in automating solutions for detecting and mitigating DDoS, which focuses on logs and traffic flow, using convolutional neural networks to learn the specific activities of DDoS traffic directly from the raw data and initiate a prediction process to decide if an attack has occurred or not. However, employees and security professionals believe that their companies might not fully involve AI, big data, or other innovative technologies in their cyber solutions.

3.1. Overview of AI and Big Data Technologies

Artificial Intelligence (AI) is an interdisciplinary field that deals with enabling computers to perform tasks that otherwise require human intelligence. AI is divided into methodologies based on the nature of human intelligence: machine learning, natural language processing, computer vision, and expert systems. AI in general, and machine learning in particular, have shown significant promise in a wide range of applications, including data mining, expert systems to provide recommendations, personal assistant chatbots, and natural language interaction, to name but a few. It is the adaptability of machine learning solutions that is driving their application in cybersecurity. This is particularly useful for dealing with security threats as these are constantly evolving.

Big data technologies offer various functionalities such as data acquisition, storage, scale-out, data fusion and management, and visual analytics. Learning capabilities include machine learning algorithms, for example, deep learning. The frontline in dealing with security threats and attacks is automated threat detection and response. Automated threat detection and response rely heavily on data interest, meaning that a data analytics platform is required for the analysis of raw data such as logs. AI and big data technologies in big data environments enable threat analysts to correlate data from different sources, reason over correlated data, and cluster/reduce false positives. Big data technologies provide a unified processing platform for data processing, analytics, and machine learning over massive data sets. Including a big data platform in an AI-cyber environment will enable threat analysts to access heterogeneous data sets and process them in near real time. It supports not only the analysis of structured data but also unstructured text data. In the field of logistics and production, organizations apply these technologies to extract data coming from radio frequency identification-enabled logistics and production systems to gain insight into potential vulnerabilities early on.

Many big data technologies have also incorporated AI technologies, which automate correlations and actions across data sets. Big data platforms have the feature of making graphs or explorations over data tables to find interesting items and actions. Also, these platforms have the capability of automation for creating exploratory models from data with the help of machine learning techniques and decentralizing the data distribution across the memory of the

cluster of machines. Another function of novel architectures includes stream and historical data processing in real time. The architecture of big data platforms inherently supports stream processing and batch processing; it is the responsibility of the user to marry historical data with real-time data processing and analytics. This will enable the threat analyst to access historical data to build a model, and when the model is built and validated, it can be piped to the real-time data streams and analytics. Real-time stream processing has become a largely used use case due to the maturity of big data platforms. As big data technologies advance, novel architectures that decentralized data storage, automate data processing, and integrate front-end algorithms attributed to big data and AI will bring about a major challenge to the cyber community, including industrial settings, which require intense national and international cooperation to tackle these challenges. The next section now discusses what we need to do to counter these challenges.

3.2. Applications in Cybersecurity

Prevalent Strategies

The increased use of AI and big data enables new styles of services and functions. This section describes several uses of AI and big data in palliative ways. The Impact of AI and Big Data on Cybersecurity

Many of the cybersecurity technologies employ an array of AI and big data solutions. The automation done by AI and big data can handle a large number of technical jobs that are often left to busy security engineers. The engineers can return to building strategic cybersecurity. If repetitive administration through AI is required, important manpower is freed to handle other parts of the work. The nature of the processing of large data sets represents trends and alerts that could be missed by CI. The definitive analysis of big data can track genuinely helpful, but otherwise indistinct and unidentified links in the CI system.

The fusion of AI and big data methods champions a new era of CI that will ensure extreme resiliency for the protection of cyberspace organizations. In addition, growing CI processes and platforms can help businesses move toward technology evolution from passive, responsive, and plan-based CI methods to dynamic approaches focused on continual progress.

AI

The use of AI is to identify viruses before they infect an organization. AI no longer requires infection to begin work on it. System managers would usually use several antivirus software programs. Virus signatures cannot be exchanged with AI upon their arrival on the server. AI can match the behavior of users with virus recognition. AI uses a blade to repel people before they ever know they are there.

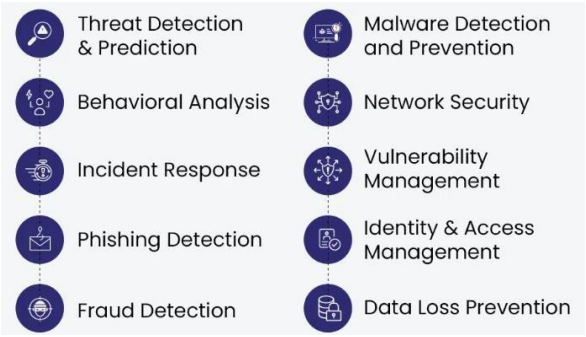

Fig 3 : Application of AI in Cyber Security

4. ERP Systems and Cybersecurity

Enterprise Resource Planning Systems and Cybersecurity Fundamentally, the purpose of Enterprise Resource Planning (ERP) systems is to assist an organization in integrating all its business processes by providing data and processes that are widely available across the organizational departments, as well as continuously redefining existing and future business norms to ensure that the organization adapts to environmental changes, including in the digital era. In addition, an ERP system acts as the brain of the organization that stores and processes information that is sensitive and confidential to the organization. Unfortunately, the very nature of data processing that supports every aspect of the organization at the code level has made ERP systems an attractive target for cyber predators in recent years. The typical four basic function modules present in ERP solutions are core management, technical, connectivity functions, and enterprise applications. A breach or vulnerability exploited in ERP deployment can harm the organization in measurable terms. ERP systems have known vulnerabilities such as weak passwords. When sunk entryways appear in ERP systems, exploitable vulnerabilities could result in the loss of information assets and various sorts of business impacts. Business impacts could include but are not limited to compromising the availability of an organization's services and myriad others regarding confidentiality, integrity, and accountability. Seeking comprehensive security capabilities for your enterprise, such as those provided by ERP ecosystem vendors or security as an add-on, is the right course to propagate operational safety. Protecting digital integrity and ensuring the availability of processing plants must necessarily be incorporated as part of your organization's strategic imperatives. Such critical systems could cause catastrophic effects at worst.

Equation 2 : Big Data Feature Aggregation for ERP Analysis

$$F_k = \frac{1}{m} \sum_{j=1}^{m} d_{jk}$$

Where

F_k: Aggregated feature value for the k-th parameter

d_{jk}: Data point j related to feature k

m: Total number of data points in the aggregation

4.1. Role of ERP Systems in Organizations

Organizations today rely on Enterprise Resource Planning systems to enrich and support a

plethora of business operations. ERP implementations integrate functions of various departments into real-time, centralized software suites and serve the diversified needs of large organizations. These integrated applications can manage and automate a wide range of back-office processes and activities involved in accounting, project management, and order fulfillment, though intelligent decision-making and reporting are among the biggest ERP benefits. The flow of successful ERP implementation is characterized by improved transparency and insights into the organization's end-to-end database, heightened accuracy due to the automation of mundane and manual tasks, and operational efficiency from streamlined processes. The use of ERP software leads to enhanced decision-making by ensuring a simpler, more manageable, and more accurate dataset is available for the generation of business intelligence and analysis reports. These systems can support millions of business processes and access vast amounts of interdependent data each second to meet the requirements of auditors, customers, suppliers, and decision-makers.

However, adopting an ERP system can be tedious and challenging; it may require dramatically enhanced attention depending on the nature of the organization, and nowadays, due to growing competition, IT threat awareness is also included. On the data governance side, well-protected and well-governed data are extremely valuable assets used by ERP systems and can affect an organization's desire or ability to effectively respond to potential threats to enhance secure use. ERP systems can be a huge source of vulnerabilities and related cybersecurity breaches. As such, numerous priorities have been suggested to help resolve and enhance the ERP implementation process, such as both organizational and personnel-level conformity. This research briefly introduces the primary features of ERP software that help organizations make efficient decisions and strengthen their data and discusses the implications and consequent thrust needed in the field of cybersecurity.

Fig 4 : AI in ERP Systems

4.2. Integration with Cybersecurity Measures

When integrating with cybersecurity measures, best practices generally state that organizations should implement enterprise resource planning (ERP) system installations securely. Also known as security implementations, companies save time, money, and breach damage by ensuring their larger data storage is not compromised. Implementations also typically involve activating security policies and user access controls, thereby limiting the number of high-privileged users on the system. In addition to initial installations, privacy, risk professionals, and security managers employ a variety of best practices and programs year-round to protect

their systems and organizations. Practices include regular updates, risk assessments, and frameworks. Additionally, many companies and computer security research professionals provide continual training exercises that enable their system users to identify and detect potential cyber threats.

Typically, these are sent out in the form of exercises and are conducted to ensure that end users recognize scams, spam, and other attacks. For years, information security and privacy companies and professionals have been pushing for organizations to take a more proactive rather than reactive stance on cyber threat detection, and it appears that now, more than ever, companies are starting to do that by incorporating software directly within large data storage servers and systems. Overall, these initiatives, tools, training, and best practices can save an organization time, money, and confidential damages. Standard cybersecurity measures also encompass various aspects of protection and are now being adapted for big data use. As such, this portion of the paper contends that plans should be developed and implemented to integrate cybersecurity within the ERP domain in settings of big data analysis and storage.

5. Autonomous Detection of Cybersecurity Vulnerabilities

The idea of cyber-physical systems capable of autonomous operation—by making decisions without the intervention of a human operator—goes back decades. However, it is in recent years that the combination of big data technologies with artificial intelligence has opened up previously unimagined possibilities. Different methodologies have been proposed for autonomous identification and protection from security vulnerabilities, but in this position paper, we focus specifically on the autonomous identification of vulnerabilities through automation of the entire vulnerability detection and response process. In large and complex systems, automation can be orders of magnitude faster and more efficient at recognizing and finding vulnerabilities than humans. This has the potential to evade adversaries before they get a chance to exploit a vulnerability and is indeed becoming a pressing requirement of due care for many regulatory regimes around data privacy, or where critical infrastructure systems are at risk of nation-state attack. Staying ahead of malicious attackers is certainly one reason, but even from a purely an operational standpoint, organizations cannot afford to employ the army of cybersecurity professionals required who might be able to provide such analysis. Various technologies and algorithms fall under this broad definition of autonomous as applied to cybersecurity. An array of operational concerns and challenges also come into play such as trust, reliability, and situational influences—context matters. To further illustrate the possibilities, we highlight some case studies. Given this, it must be emphasized that for organizations to have any hope of staying ahead of their adversaries, they are compelled to have some level of automation built into their rapidly evolving cybersecurity perimeter and procedures. This is a practical anachronism, as without such capabilities, they will find themselves overwhelmed by scale, speed, and complexity.

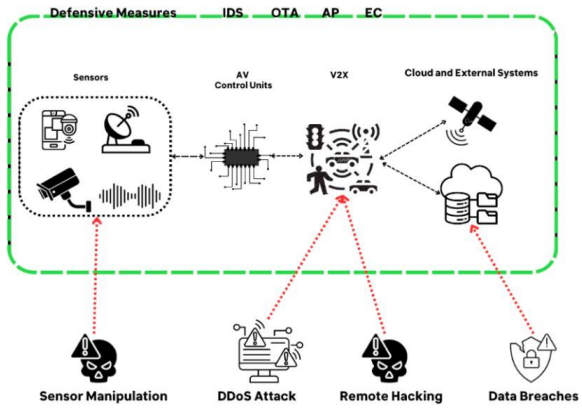

Fig 5 : Cybersecurity in Autonomous Vehicles

5.1. Concept and Benefits

Definition: The term autonomous means with or without the control of humans, and such systems are powered with the ability to make decisions and operate by themselves. In cybersecurity, autonomous detection means that an automated system is used to detect threats in the network or a computer system using artificial intelligence techniques. In this essay, we focus on an autonomous detection system for the detection of cybersecurity vulnerabilities to protect the system from being attacked. The major significant benefit of an autonomous detection system over traditional manual detection methods using human operators is the accuracy of detecting vulnerabilities. Furthermore, an autonomous detection system can detect vulnerabilities in a real-time fashion, unlike a human operator who takes a considerable amount of time to find and detect threats in the network. Autonomous detection systems are operated using intelligent algorithms and machine learning techniques, which decide to take actions according to the current state of the threat in the system. Moreover, such detection systems will machine-learn, and their accuracy level in detecting vulnerabilities increases as time passes. Autonomous detection systems are operational all the time, providing constant detection of vulnerabilities in the network, immediately after they appear in the system without any stop. In addition to that, such systems are non-fading and prevent human operator fatigue during the performance of their operations. Autonomous detection systems are efficient in terms of cost because they do not require a large amount of investment, such as securing well-trained and skillful operators. The growth in the development of decentralized and autonomous technologies is essential as it paves the way to manage highly decentralized threat vectors and battle cyberattacks. An autonomous detection system can be easily deployed into any virtual network environment because of its software-defined nature of deployment. Moreover, its unique features allow it to be integrated with existing cybersecurity detection hardware and software products to enhance their effectiveness in cybersecurity threat detection.

5.2. Case Studies and Examples

Implementations and Case Studies. This section shows practical illustrations of autonomous detection systems. Autonomous detection of system vulnerabilities has been implemented through ERP and big data systems across many different types of companies. Some of these include a seminal early adopter from the financial services industry, a semiconductor

manufacturer, a direct-to-consumer internet retailer, and a global leader in the toothpaste market. Each case represents a separate revolutionary approach to applying autonomous detection for system vulnerability. In each example, we executed a virtual proof of concept in a historical context. The results from these cases were documented as those new systems became operational. Overall, clients experienced the benefits expected from a reduction in cyberattacks as their systems were patched before the general public was widely aware of system vulnerabilities.

In each case, as new technologies became more readily available, we noted the benefits, challenges, and lessons learned. This paper's lessons were used as inputs to each case, typically by adapting them for specific product managers and other team members. We expect there to be a significant learning opportunity that can be deployed when autonomous systems more widely detect threats. In our experience, additional breaches and real threats are found when detection systems are used in conjunction, including those that are very recently deployed and do not have the typical trails of breadcrumbs that may be found in older system logs. Consulting with the business through vendor reviews, risk assessments, and other tasks is needed to monitor the degree of success in reducing threats.

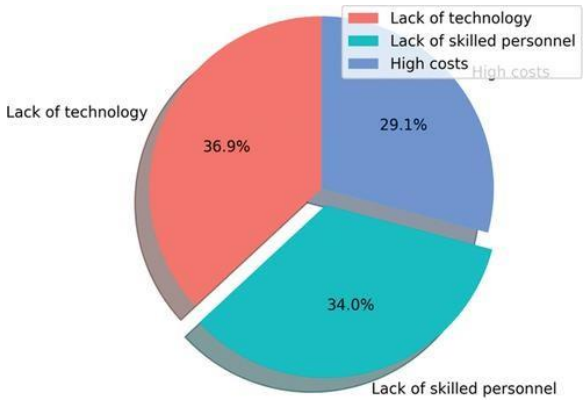

Fig 6 : Current trends in AI and ML for cybersecurity

6. Challenges and Ethical Considerations

The enabling and delivery of advanced cybersecurity technologies are also likely to face ethical and governance challenges. The leverage of AI and big data potentially entails data privacy and ownership issues, as they create the potential for vast datasets to be gathered about an autonomous ERP system that is scanning the internet for information on a given target. These datasets may hold significant intrinsic value, in terms of knowledge leadership, for the organization and also present opportunities for the reselling or licensing of the data as a non-market advantage. Issues of responsible data use may also arise about data protection regulations if these gathering processes are massively deployed without the consent of the data subjects, who will likely be unaware that their data is being gathered. The increasing development of AI and machine learning also increases the potential for AI to be employed in decision-making processes. This may present particular issues about accountability, including the use of AI in decision-making that may have serious consequences, as well as the difficulties

of developing transparent systems through which the reason for a decision can be identified.

Ethical frameworks are needed to guide the use of AI and big data in security applications. Specific ethical issues include unfair treatment and bias discrimination; transparency and accountability; privacy; and security. In the cybersecurity context, AI systems could potentially exhibit bias by favoring particular users and applications above others, similar to the risk of bias associated with employee security vetting. Security algorithms and protective measures that have indicated bias or discrimination against a group of users have a net negative security effect due to the marginalization of the population concerned. There are efforts in the industry to find software solutions to detect bias with security algorithms. The sensitivity and security challenges of this type of research impede the ability to get a full picture of the type and extent of the approaches being explored. Throughout the advancement of new technical security initiatives, there needs to be careful research and discussion of the ethical implications and real-world operationalization of change. This will facilitate informed debate and ensure that the operation of the ethical and legal frameworks can keep pace with the latest technological developments while safeguarding people, organizations, and networks. The existing ethical and governance challenges specific to AI and big data are therefore key considerations in public and private research that aim to include automated vulnerability detection in future systems to address global cyber challenges. This should not, however, prevent or delay technical advances in this space to ensure an appropriate balance of ethical and technical considerations.

6.1. Data Privacy and Security

In an era of cloud computing, AI, and big data analytics, data privacy becomes a critical issue. Along with numerous benefits, ERP systems have also brought challenges for industries in securing sensitive and private information. With the large-scale collection, storage, and processing of data, complete data security seems impossible. There are various numbers of attacks launched through AI to bypass cybersecurity measures. To prevent and counter such attacks, organizations may be required to reinforce the traditional way of securing information through the implementation of AI-driven data security measures. In the current case, a European company may have to adhere to stricter regulations. To protect users and their private information in AI-driven big data technologies, industries are also required to consider ethical norms. This approach may help to protect users' rights against potential algorithmic biases, intentional or unintentional data corruption, and unauthorized sharing of sensitive data among third-party interest seekers and intermediaries.

The use of advanced data security technology in AI can help facilitate the industry's practice toward adaptive and flexible security policies. Thus, governments and related departments can use AI-driven big data technologies to illustrate and sustain adaptive data security policies. AI can be made to learn and recognize hidden patterns, intelligently predict abnormal logins, and restrict unauthorized access by using standard deviation, Pearson correlation, and other clustering and discriminant analysis techniques to differentiate the trend of genuine users from abnormal users. On the other hand, AI also carries the risk of revealing harmful criminal behaviors and data breaches by intelligent users. Companies using big data analytics and AI can uncover any hidden or suppressive tactics employed by hackers to breach fundamental network firewall systems. Since all the major advances in technology have a few

consequences, the enormous potential of big data collected and analyzed via AI may also raise ethical concerns. Used ethically, it has enormous potential for creating an innovative landscape. To configure the hybrid threats, legal and regulatory measures need to be strengthened.

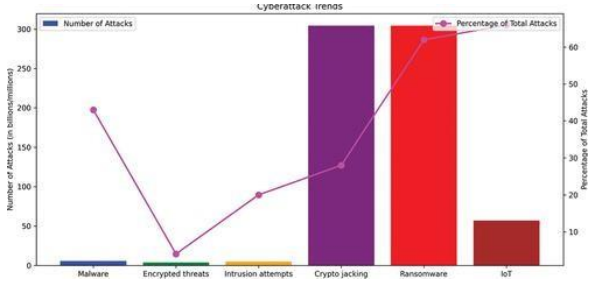

Fig 7 : Present Cyberattack trends.

6.2. Bias and Fairness in AI Algorithms

AI systems are designed to learn from data to create models that can identify patterns and make predictions. However, even data can contain biases. For security systems, this is a considerable challenge, and discriminatory effects could lead to a detrimental impact on cybersecurity. Algorithms trained on biased data can perpetuate unfair biases, providing differential care or protection to various populations. In contrast, they can put different groups of people at risk of cyberattacks due to the biases in trained AI systems. This can result in an unequal distribution of risks, online harassment, identity theft, and loss of digital privacy, along with many other harmful implications. Fear and uncertainty related to unfair bias and the discriminatory nature of AI can lead to a refusal to trust AI in security measures. This is particularly important in AI-based security systems where decisions are irreversible, and millions rely on them.

Methodologies for identifying and minimizing unintentional biases that are embedded within AI algorithms are still in the development phase. Yet, different strategies can be considered as a blueprint that helps to build fair algorithms. One such approach is through the development of transparent and interpretable AI algorithms that not only identify the bias but also indicate the potential legal, social, and ethical implications of the bias through the decision-making process. This can result in the compatibility of AI systems with the principles of accountability, fairness, and equity. This means that decision-making processes are transparent and subject to public scrutiny if taken reliably and capably. This approach is defined as fairness through awareness. Another approach to making AI algorithms fair is to integrate every aspect of the affected human's scope into the AI training data. Deep, wide, and diversified data are essential to prevent the production of detrimental results. In other words, having access to diverse predictions aims to create inclusive big data. Furthermore, another approach is to use legal instruments to develop a protective mechanism against the biases created through AI algorithms. Therefore, advanced legal settings that take into account the ethical and fair risks can be beneficial in addressing the issue of bias in the security of AI.

7. Future Directions and Conclusions

We have reviewed and analyzed relevant research to understand how AI-powered big data and ERP systems can be integrated to develop a cohesive security solution for detecting cybersecurity vulnerabilities. We conclude that our proposed framework is a beneficial and innovative solution to address the aforementioned cybersecurity vulnerabilities. The current threats are targeting the connected world. Moreover, sensor devices and remote control analysis for understanding data patterns can trigger a lot of insights into the connected world.

Future Directions

This solution can be further operated in an unstructured environment by including AI for recognizing the intelligence of the attacker's footprints. Our proposed security framework can greatly help in improving the present world of cybersecurity surveillance. Furthermore, in the future, with the increasing use of drones and unmanned automated vehicles, such end-to-end surveillance monitoring solutions can be a major benefit for future populations. People also have to be trained and motivated more to adopt intelligent devices because most of the devices will be remote and people won't have direct control of them. Countries and organizations can increase their protection by embracing the significant technologies of the present day. The organizational processes can be better equipped for the incoming threats in the future. The continuous monitoring of cybersecurity further ensures the current state of an organization's security. Together, while AI and big data have a lot more evolutionary directions, education, and research should be in that direction, thereby increasing the nation's and global system's cost and value. The complete roadmap helps in building an intelligent network to address newer cybersecurity issues. In addition, economies must also concentrate on smart cities, intelligent vehicles, and intelligent health systems. An economic bolster may also need to be continued in this area. The public and private sectors must work together to construct a robust security system as a unified force.

Equation 3 : Risk Prediction Through Gradient Boosting

$$P_t = \sum_{l=1}^{L} \eta \cdot h_l(X)$$

Where

P_t: Predicted risk level at time t

η: Learning rate

$h_l(X)$: Output of the l-th weak learner on big data X

L: Total number of learners

7.1. Emerging Trends in AI and Big Data for Cybersecurity

Rising volumes of advanced persistent threats along with zero-day vulnerabilities are now pushing security professionals to rethink existing cybersecurity paradigms. By and large, data and predictive analytics will provide intelligence to anticipate and counter security threats. While AI and big data technologies can provide several potential applications that could be directly or indirectly leveraged and exploited for enhanced cybersecurity applications, developments in the domain of AI, big data, and cybersecurity are also contingent upon many future directions that involve physical, social, economic, and legal implications. Advancements in machine learning domains, such as natural language processing, extend state-of-the-art analytical capabilities for improved auto-classification of security

vulnerabilities. Foundational and developmental predictive analytics can now be conducted using big data.

Predictive analytics enable rapid, automated identification of patterns and improved decision-making. Concurrently, endeavors are underway to evolve existing cyber threat analysis practices into a cybersecurity aspect of big data science to accommodate the scale, complexity, diversity, and variety of data relevant to cybersecurity. Ongoing research in AI is already providing solutions that enable AI learning to dynamically anticipate AI systems to have increasingly shared intelligence in a collaborative environment. This relatively novel approach to AI learning can be exploited in the domain of cybersecurity possibilities in terms of AI egotism. Furthermore, there has also been a sharp rise in ethical AI systems that focus on principles or values in AI systems to ensure fairness, equity, or accountability. Evolutions in AI and big data for security offer organizations the potential for enhanced vulnerability detection and response. Though still nascent, staying abreast of future trends in AI and big data for prognostic innovation on the global stage is essential for cybersecurity strategies and practitioners.

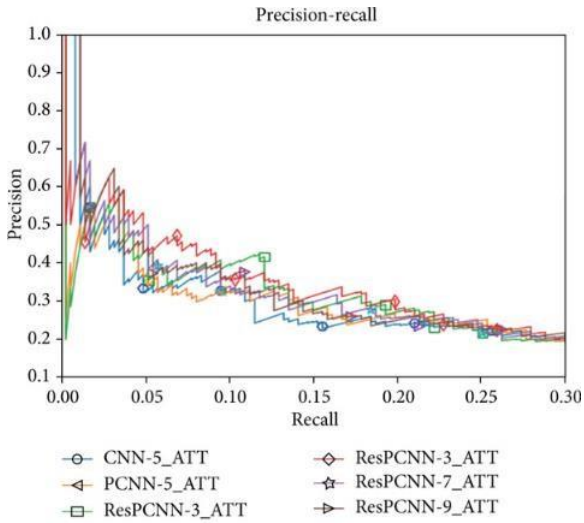

Fig 8 : Data-Driven Cybersecurity Knowledge

7.2. Key Takeaways and Recommendations

7.2.1. Key Takeaways

1. AI-powered big data and ERP systems can autonomously detect, classify, and mitigate cybersecurity vulnerabilities before they are exploited by bad actors.

2. Information security is only as strong as the technologies that underpin it; organizations and government agencies should consider integrating these advanced approaches into their information security strategy.

3. As the use of AI and big data impacts every aspect of daily life, ethical arguments, and information must comply with relevant federal policies and regulations. To accomplish this, the organization should fully integrate the use of a big data ERP system within its information

security program.

4. Regardless of the AI-driven future of information security, maintaining an incident response team is vital to immediately respond to all cybersecurity incidents. This team will address all potential cybersecurity hazards that the AI-driven big data system may miss.

7.2.2. Recommendations

1. Enhance data management, analytics, and reporting principles within existing programs and projects.

2. Boost training in critical data analytics to focus on detecting technical lagging and current threats, including threat chains from perimeter threats, hacktivists, advanced persistent threats, and cybercrime organizations.

3. Develop a plan to compare internal knowledge, skills, and abilities with the speed of learning and detecting technologies.

4. Prepare the Board and CEO to communicate the plan to monitor and periodically assess the current cybersecurity risk evaluation, desired state, and relevant key risk indicators.

5. Invest in regular technology tests and exercises to ensure system effectiveness.

6. Obtain assurance that legal and regulatory privacy issues can be continually addressed.

7. Follow a continuous improvement program that embraces adaptive learning and changing practices as the threat evolves.

References

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

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

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

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

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

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

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

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

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

[10] Siddharth K, Gagan Kumar P, Chandrababu K, Janardhana Rao S, Sanjay Ramdas B, et al. (2023) A

Comparative Analysis of Network Intrusion Detection Using Different Machine Learning Techniques. J Contemp Edu Theo Artificial Intel: JCETAI-102.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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