UtilitasMathematica
ISSN 0315-3681 Volume 121, 2024

Predictive Analytics and Big Data Integration for Strengthening ERP Systems Against Cybersecurity Threats

1. **KishanKumar Routhu,** ADP, Senior Solution Architect

2. **Suneel Babu Boppana,** iSite Technologies, Project Manager

3. **Krishna Madhav Ja,** Topbuild Corp, Sr Business Analyst

4. **Vasu Velaga,** Cintas Corporation, SAP Functional Analyst

5. **Varun Bodepudi**, Deloitte Consulting LLP, Senior Solution Specialist

6. **Laxmana Murthy Karaka,** Code Ace Solutions Inc, Software Engineer

Abstract

This paper contributes to and extends the existing literature on the importance of predictive analytics within Enterprise Resource Planning (ERP) systems by providing a holistic view of potential threats and optimal mechanisms associated with their implementation. However, this study is not a panacea, as it admits that achieving the aforementioned objectives presents a considerable challenge. We claim that academic researchers, developers, companies, regulators, and lawmakers must enter into a collaboration scheme that enables the development of the best designs of predictive models and integration strategies of Big Data into ERP systems.

Nowadays, as the numerical output exceeds the analytical capacity of many ERP users, predictive analytics help to convert raw Big Data into valuable and easily understandable strategic information in real-time. The goal of this paper is to describe the benefits associated with predictive analytics and Big Data quality. Additionally, we introduce a conceptual model to demonstrate how Big Data can be integrated into ERP, increasing the robustness and resilience of both predictive analytics about the occurrences of potential threats and the correlates, alerts, and responses.

Keywords: Predictive Analytics, Enterprise Resource Planning, ERP Systems, Big Data, Integration Strategies, Holistic View, Potential Threats, Optimal Mechanisms, Collaboration Scheme, Predictive Models, Real-Time Information, Strategic Information, Big Data Quality, Conceptual Model, Robustness, Resilience, Potential Threats Occurrences, Alerts, Responses, Analytical Capacity.

1. Introduction

Information systems, in particular enterprise resource planning systems, stand at the core of business operations in organizations, offering support to process critical activities and supporting business objectives. In a digital world, organizations are undergoing digital transformations to integrate technology into all aspects of their operations and customer interactions, embedding digital capabilities in their products, services, and core business processes to increase their customer experience and meet global challenges in a quickly evolving marketplace. The demand for digitalization from businesses has tripled in the wake of the pandemic with associated growth, accelerated cloud adoption, and the expanding digital landscapes. Amid a hybrid workplace environment, ERP systems are now expected to deliver real-time omni-channel customer services and seamless employee experiences through mobile, social, cloud, and big data technologies. However, the multidimensionality of emerging complex environments with greater connectivity and the synergistic digital policies and corresponding systems infrastructure needed to provide secure, reliable, resilient, and sustainable ERP operation are still fundamental topics meriting critical inquiry.

1.1. Background and Significance

Cybersecurity of large enterprise systems is vulnerable because such systems are highly monetarily and information-sensitive targets situated in varied dispersed and non-dispersed geographies. They are defenseless due to multiple levels of interaction points that could be accessed by numerous computing devices using wired and wireless data transfer protocols, while the real guard points are limited in number and cover only the strategic or, to some extent, the major points of the system. Lately, increasingly reported cases of cybersecurity breaches and incidents along with their proven financial effects are encouraging companies and governments to increase efforts and allocate resources

for enhancing their ERP systems' cybersecurity.

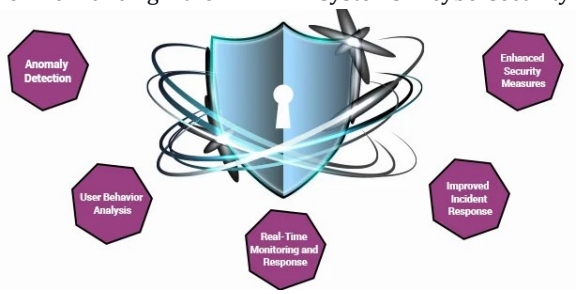

Fig 1 : Cybersecurity Predictive Analytics

Organizations right now are saturated with tremendous amounts of structured data archives inside their data reservoirs or data ponds. In the realm of information technology, the term "Big Data" is often, but not always, an indication of humongous volumes of data items. It is further defined as high-speed in capturing, querying, and interpreting meanings, and has a variety of data source types encompassing structured, semi-structured, and unstructured data. Big Data also often needs access to real-time or near real-time modes to match the speed of today's quickest speed demon race cars. Big Data is not solely large, but also complex and challenging the norms for processing, storing, and interpreting data items with the aid of classical database terms and concepts related to structured datasets. To sustain their cybersecurity mission by constantly detecting with greater precision the menace of turmoil in their information repository, software products that perform predictive analytics have been enhanced to tightly integrate the advantages of the Big Data approach to the cybersecurity domain.

Equation 1 : Predictive Risk Scoring

$$R_t = \sum_{i=1}^{n} w_i \cdot f_i(x_t)$$

Where

R_t: Risk score at time t

w_i: Weight of the i-th predictive feature

$f_i(x_t)$: Function evaluating the i-th feature at time t

n: Total number of features

1.2. Research Objectives

The specific objectives of the research are described below. Literature Analysis: To establish theoretical and research bases on the usage of big data and predictive analytics to increase the cybersecurity of enterprise information systems. Analysis of the Modern State of Enterprise Resource Planning Systems Cybersecurity: To examine the modern state of enterprise resource planning systems cybersecurity in the context of their stakeholders, typification of information risks, protection from unauthorized access, protection from data destruction and blocking, protection from service disruption, and analysis of the existing enterprise resource planning systems security solutions for these components. Development of the Model for Strengthening ERP Systems Against Cybersecurity Threats: To develop an energy-efficient, cost-effective, easily implementable, and enforceable model for strengthening ERP systems against cybersecurity threats. Classification of External Monitors of the Strengthening IT Infrastructure of Enterprises for Cybersecurity Threats: To perform classification of the external monitors of ERP systems for cybersecurity threats and to justify further research on the communicative contexts attitude. Optimization Criteria and Efficiency Evaluation of Software for Strengthening and Managing Cybersecurity Threats: To choose a multi-criteria assessment model of the software for the management of ERP cybersecurity threats magnitude according to their predictive indicators, and to evaluate the performance improvement by the integration of big data processing software, as well as its adaptation for specific communicative contexts under consideration. Development of the Information Security Model of the Enterprises: To present an example of the informational-analytical software-related solution and performance outcome argument for the development of big data-based or enriched solutions to enable software for all types of internal and external communications, supporting the accounting of the social context that may enforce a revolutionary breakthrough for computing power usage efficiency in question and a designated self-learning model.

Fig 2 : Unleashing the Power of Data Analytics in Cybersecurity

2. Theoretical Framework

The combination of predictive analytics and big data will give a stronger cybersecurity system and is also a wise improvement for existing ERP systems to be much denser in countering a broad range of cybersecurity threats. The increasing number of threats to information technology security is truly alarming. The level of security attacks conducted on a large number of IT infrastructure companies is also varied, and almost every time they are innovated. These real conditions become a sort of call for researchers and practitioners to remain aware of all the important aspects presented by cyber threats on many companies both now and in the future. Attackers always come up with different strategies to analyze various systems; therefore, researchers are required to act proactively in dealing with new threats and new variations in old threats to anticipate their occurrence. Thus, in its development, researchers continue to put in a lot of effort to build a solid and strong guard against the dangers faced by the vast world of IT.

Current analysis of cyber attacks is still commonly conducted a long time after the cyber attack has occurred, and this condition does not provide an opportunity for the company to immediately minimize the chances of future cyber attacks and may even anticipate these conditions. This research is very beneficial to all parties. Companies do not have to wait until an attack occurs to take steps to address it. Researchers can try out curative model theories through certain testing of research. The same can be done in the analysis of cybersecurity in IT. In recent years, IT managers have been facing threats from various cybersecurity attacks that can be detrimental to an organization, such as loss of data, systems, service stability, and even financial losses and a damaged reputation. Mastering the dimensions of the victim and attacker in the security system will increase understanding and effectiveness in tackling and developing a more organized IT security strategy.

2.1. Predictive Analytics in Cybersecurity

Predictive analytics represents the capability of scanning large sets of data to extract information and develop models that can be used to predict future events and actions. It is a proactive examination of digital communications that can make a difference in many fields such as marketing, retail, healthcare, manufacturing, and security in general. Predictive analytics happens thanks to technologies and statistical techniques that are used in the field of machine learning, typically data mining, statistical algorithms, analyses of latent variables, and advancements in data technologies. Specific fields of application for predictive analytics are represented by cybersecurity alerts, risk evaluation, threat prioritization, fraud detection, and so on. Particularly in predictive asset maintenance, if applied in actual fashion, with true predictive analytics models, enterprises could save billions and workplace safety could be highly increased. In the field of cybersecurity, predictive analytics can ascertain attacks that will occur with a certain lead time.

In information technology nowadays, cyber threats represent a complex situation. As people and activities have become digital, cybersecurity risks have continued to grow. Fundamentally, the problem of cybersecurity is due to the usage of technologies different from those that enable them. Society is currently spending more on cybersecurity than ever before, yet the attacks and breaches show a strong upward trend. The usage of technology to carry out criminal activities and the opacity of the technology operations are the main reasons for this fact. Cybersecurity seems to be more of a problem intrinsic to the technology than any other consideration. Companies have accumulated large stocks of digital information in segmented customer and credit card databases. Cybercriminals break into networks using malware that is only after credit card and customer data to resell. The variety and quantity of cyber data trigger the use of new decision methodologies. The use of predictive analytics to decide about the use of cybersecurity countermeasures is relatively new. Nonetheless, it might be the best way to decide because we are dealing with a niche problem and we aim to detect attacks earlier to prevent most of their fallout.

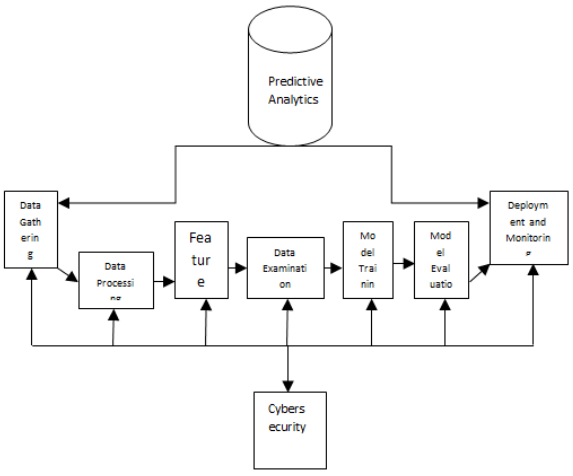

Fig 3 : Predictive Analytics Framework for Cybersecurity

2.2. Big Data Integration in ERP Systems

Big Data refers to a large volume of data in petabyte and terabyte sizes and the exponential growth of Big Data achieved by the digitization of computing technologies.

Volume is not the only defining characteristic of Big Data, nor are velocity, variety, veracity, and value solely defining elements of Big Data. The 4Ps of Big Data define that the existence of Big Data is demonstrated by its four characteristics: volume, velocity, variety, and veracity. Many open-source social media platforms help consumers easily share their experiences on products, recommendations, wish lists, consumer reports, and discussions across many topics. These inputs serve as treasure troves of unstructured data offered through various content types such as text, images, videos, numbers, and also social media activities or network relationships. Many organizations, to manage their business operations efficiently at a lower cost, often prefer an integrated suite of Enterprise Resource Planning applications. Consumer interaction and feedback are essential elements for improving the quality of offerings and for refining product and service direction. Social media services create new opportunities for businesses to enhance customer engagement, monitor the performance of services, and assess the quality of products. Estimating web opinion propagation dynamics is very expensive in terms of business operations. Integrating social media techniques and marketing strategies with ERP systems provides benefits to maximize customer engagement activity. Big Data decision analytics deal with predictive algorithms and descriptive models. Descriptive models are nothing but outcome prediction processes employing machine learning algorithms. These models describe and predict various aspects of data trends, associations, behaviors, and complex structures of data conveyed and controlled by the interactions of users with ERP applications.

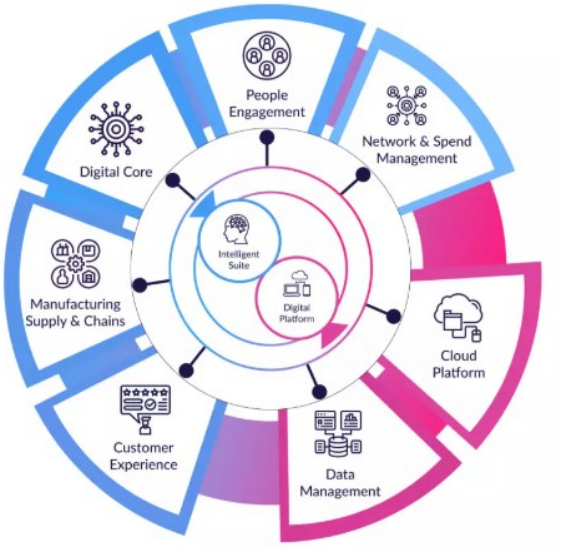

Fig 4 : AI in ERP Systems

3. Methodology

This chapter describes how the particular methodology integrates and calibrates the available complex predictive analytics techniques, data mining tools, and big databases to assist organizations in strengthening their Enterprise Resource Planning systems against cybersecurity threats. Furthermore, throughout the description, the necessary instruments are reviewed. To achieve this, the possible predictive analytics and big data tools useful for such a case should be thoroughly reviewed. Then, the rationale, methods, and necessary mechanisms to combine them are presented. The suggested methodological approach can be deployed in any type of organization, and relevant guidelines, additional tools, drawbacks, and unique capabilities are provided.

The applied research, achieved results and used instruments—predictive analytics and big data tools—should be carefully described. This is a very important step, especially when organizations seeking assistance to implement the same proposal come from entirely different industries. The role of the applied methodology in terms of predictive analytics is seen as connecting all available techniques and tools with the available data, optimizing the usage of various methods depending on the best outcomes achieved, and operationalizing the generated results and predictions for a minority of non-IT experts. The review of the proposed methodology should also include a comparison to existing ones and the advantages of its application. At the end of this chapter, the adopted measurement instruments for checking the satisfaction of the study objectives are also presented.

Equation 2 : Anomaly Detection using Statistical Thresholding

$$A_t = \begin{cases} 1, & \text{if } |x_t - \mu| > k \cdot \sigma \\ 0, & \text{otherwise} \end{cases}$$

Where

A_t: Binary anomaly flag at time t

x_t: Observed system metric

μ: Mean of the metric under normal conditions

σ: Standard deviation of the metric

k: Sensitivity threshold

3.1. Data Collection and Analysis Techniques

There is an exponential increase in the amount of data generated in an organization with Global Information

Systems and other enterprise software. In ERP, advanced analytic tools can be incorporated to unlock the trends in the data. The use of business intelligence combined with GIS products and best practices can help in using the data from a variety of sources and produce valuable insights. Some of the techniques that are used in analytics, such as descriptive analysis, predictive analysis, and prescriptive analysis, can be used for access control mechanisms. Descriptive techniques can be used to detect problems in current access controls. Predictive techniques can identify the problems at a future point in time. Prescriptive techniques can suggest appropriate improvements to access control policies. They can also make advanced predictions and, at the same time, provide recommendations including main indicators.

Descriptive analysis is the bottom-most level at the detailed raw data level. It is used to summarize and describe the characteristics of a set of data and to clearly define the size and the structure of attributes. Predictive analysis is an analysis of different attributes but never consists of the actual optimization of features. It is used for more accurate predictions, as data is never perfectly informative. Predictive analysis is followed by optimization. Predictive characteristics of unauthorized access behavior are to be implemented within the business application with extensive new data with a label model that defines specific rules that are followed for such prediction. Unauthorized access behavior within the enterprise software can be detected by monitoring business data access patterns. The various techniques to detect the issues are by using traditional analytical systems that are in operation or are using the new continuous controls monitoring systems that mine business applications continuously. A lot of research concerning enterprise software has also shown different business process patterns that are being followed, supporting business access patterns.

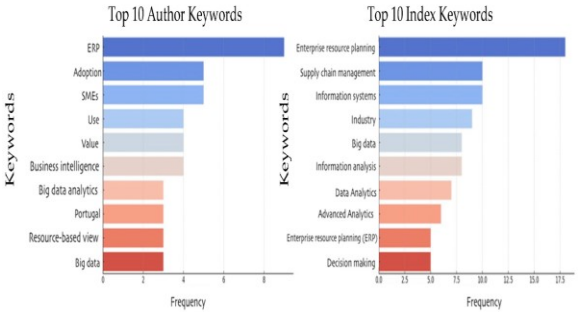

Fig 5 : Integrating Analytics in Enterprise Systems

3.2. Case Study Design

One critical concern for the design of a case study aimed at predicting, preventing, and mitigating user threat exploits to ERP systems revolves around data access and availability. Cybersecurity datasets are in extremely high demand in the academic and private sectors due to the critical nature of the topic. There are a few main challenges and limitations that prevent or limit access to such valuable data. Through partnerships with vendor sources and existing freely accessible large federal repositories, there can be access to a multitude of datasets, but certain aspects are protected by either being restricted or having cost-based access. Through the use of the provided environments' user workstation, as a controlled third party, the opportunity to apply predictive analytics research solutions to help quantify the risk of identified threats and provide tested and verified methods digitally maximizing the ROI of investments made in cybersecurity protections is made possible using this information. However, despite the partnership, access to a more complete relational schema for analytic model creation, specifically in the ERP system utilization scenario, was limited in this case.

4. Findings and Discussion

The survey consisted of questions providing six respective dimensions of PABDI. The preliminary survey and interviews to determine the perspectives of the consultants, software engineers, and cybersecurity specialists in enterprise systems allowed the structuring of an instrument based on the objectives given. In the research model, 37 survey items were retained for further analysis. The data was analyzed by procedures like exploratory factor analysis, confirmatory factor analysis, and structural equations modeling to determine the proposed model's relationships between the study's constructs. The current study is future-oriented, mainly focusing on cybersecurity weaknesses and how the predictive analytics capability can be maximized to benefit the organization's cybersecurity performance.

The findings demonstrate that big data integration into ERP represents significant capabilities to overcome cybersecurity threats, and predictive analytics power directly influences these capabilities. The survey provided such an extraction pattern as ERP big data integration composed of seven dimensions, and predictive analytics denoted as business pre-advance value. Furthermore, cybersecurity is considered part of ERP architecture, concerning ERP/BI processes surrounding the economic and non-economic territories. Finally, the predictive capabilities of the organization result in a wider model of creating a database that stores unknown items. In addition, the PABDI-directed accompanying dimensions are expected to enable an

organization to directly or indirectly increase the results of other ERP/BI functionalities.

4.1. Impact of Predictive Analytics on ERP Security

Predictive analytics deals with the use of statistical and scientific methods for analyzing current and past data sets to determine patterns, foresee future trends and forecast outcomes. Predictive analytics can be applied using many different tools, such as artificial intelligence, data mining, and statistical modeling to understand the latest trends and predict the effects of approaches to a given problem. As a result, for an organization to detect and mitigate a cyberattack, it needs to know about the latest cyber risks, including new attacking methods and the propagation of specific threats. Predicting cyberattacks and protecting ERP systems against potentially harmful incidents, such as unauthorized access to data, modification or destruction of important data, or the reduction of resources, will allow the organization to provide the highest level of security.

The kinds of data types and sources of information that ERP systems, especially those used in production tracking or supply chain management, process are unfortunately increasing, which, in turn, increases the possibility of a serious external threat, such as destructive cyberattacks. Additionally, the use of large databases and servers makes ERP management more vulnerable to performance issues and security vulnerabilities. As a result, an organization's sensitive business rules and financial data can be accessed by malicious users from different sources using various channels, such as system maintenance, emails, and the Internet. Today's well-developed technologies are unable to keep up with the deployment of most ERP systems; specialized precautionary approaches and protection mechanisms have provided inadequate security control. Consequently, organizations are unable to provide sufficient security by only relying on internal safety mechanisms that already exist. Therefore, to strengthen the security of ERP systems, organizations need to use specific new models that will immediately detect and mitigate potential cyber threats. When these models demonstrate that security is insufficient, the organization can increase security through the most current safety mechanisms.

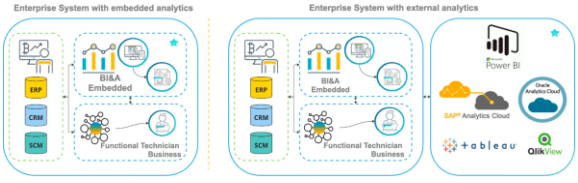

Fig 6 : Enterprise systems with embedded or external analytics—own elaboration.

4.2. Role of Big Data Integration in Cyber Threat Detection

The huge number of vast and sophisticated demands is today used by potential attackers to steal sensitive data, promote ransomware, steal privacy, or damage or interrupt business functions. To safeguard and handle these potential dangers, firms are increasingly embracing big data and analytics. Big data supposedly includes technology and methods to handle substantial amounts of varied types of information. Currently, cyber threat identification depends mainly on signature-based schemes. Using the signature matching of known threats to defend systems and networks, signature-based systems compare new data with a database of patterns. But to safeguard the networks, these conventional recognition technologies are not powerful. Once a fresh danger is found and there is enough data to produce a model, even machine learning-based solutions could just forecast new potential cyber threats. The next cyber danger can compromise business activities or internet suppliers until the model is developed with complete information and is appropriately confronted. The primary architectures for examining these massive datasets created for these purposes are the distributed architectures and platforms that are a component of the big data system.

5. Conclusion and Future Directions

This paper refers to a cyberattack prevention system developed using a predictive model to predict zero-day cyberattacks. We refer to the architecture of the system and the individual blocks, libraries, and databases used. Furthermore, this paper includes a practical test of the prevention system using real zero-day cyberattacks. The resulting test dataset is used for machine learning predictive models to evaluate the prediction outcome in terms of the accuracy of the cyberattack prediction. This system aims to prevent zero-day cyberattacks as early as possible. We used predictive model-based trends to predict zero-day cyberattacks 10 days ahead of the present day using both significant features and non-significant reduction feature subsets input to the predictive model. Furthermore, we implemented the system to work and tested it with an existing antivirus. The validation of the system was conducted in a real environment using available and real zero-day cyberattacks to obtain the various and most relevant datasets.

In the future, the system for preventing zero-day cyber attacks will be upgraded with a fully automated updated input dataset for both a training dataset and a testing

dataset. The upgrade of this system will also include the algorithms used and parameter tuning. Further research is needed to specify the features of the datasets in the field of machine learning, and also further investigation and analysis of the simulated test. Furthermore, future work should check whether the timeframe of the implemented zero-day prediction system could be extended to ensure that organizations are better prepared against potential threats. Future research should consider the many other stages of readiness and recovery for other potential cyberattacks. Furthermore, based on priority, the next system to build is a tool that might reveal potential system vulnerabilities to cyberattacks using IoT. This research has opened the door to the potential combination of predictive models for the prevention of network security hazards and will be analyzed in future research.

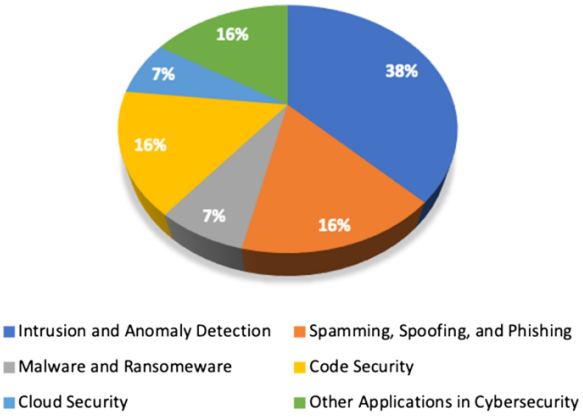

Fig 7 : Big data in cybersecurity

5.1. Summary of Key Findings

This chapter has analyzed how we can strengthen big data and predictive analytics within enterprise resource planning systems to combat cybersecurity threats from both internal and external attackers. The analysis has shown that in the last three decades, there has been a lack of consideration for predictive analytics and big data in strengthening ERP systems against cybersecurity threats. The study shows that big data and predictive analytics are new areas within ERP systems that need to be adapted for advanced cybersecurity deployments. Furthermore, big data and predictive analytics are well-known for combating internal threats in various systems. However, they are not given the same intensity in the context of ERP systems. In practice, predictive analytics and big data are established as separate subsystems from ERP systems. This is a result of the fact that in organizations, data are primarily generated from both enterprise resource planning systems and customer resource planning systems. When these databases are extended, additional computing and maintenance costs are incurred in terms of both hardware and software systems. Hence, creating a separate general data system may be more cost-effective than managing comparable functionality using existing enterprise systems.

Equation 3 : Big Data Integration Correlation Model

$$C_{ij} = \frac{\mathrm{Cov}(X_i, X_j)}{\sigma_{X_i} \cdot \sigma_{X_j}}$$

Where

C_{ij}: Correlation between big data streams X_i and X_j

$\mathrm{Cov}(X_i, X_j)$: Covariance between X_i and X_j

$\sigma_{X_i}, \sigma_{X_j}$: Standard deviations of X_i and X_j

5.2. Recommendations for Future Research

This research represents an initial attempt to model and forecast possible security threats in ERP systems. We believe that there are still many areas for improvement in this proposed model. In particular, we think there are still other variables that might have a greater influence on the dependent variable. One passive way to collect attack information is to deploy a kind of software that is meanwhile executing different types of processes. The only necessary information is the log file of the entire process. In a corporation that has the dimensions to bear huge numbers of virtual machines, perhaps this wouldn't be an impediment.

We believe future research can design a smarter way to exploit this data source. In the method presented in this research, only capabilities of this kind of access are ranges over the network using some network layer protocol. However, with a huge data set of malicious attempts and data consisting of ranges on the net, and the log of the systems as output, we think that data mining techniques and regression techniques will extract normal ranges that perhaps would be used more efficiently to discover vulnerabilities, which windows could be easily cracked. We must stress that we don't speak here of penetration testing but of the actual use of the system generating useful data that does not grow constantly.

6. References

[1] Ravi Kumar Vankayalapati , Chandrashekar Pandugula , Venkata Krishna Azith Teja Ganti , Ghatoth Mishra. (2022). AI-Powered Self-Healing Cloud Infrastructures: A

Paradigm For Autonomous Fault Recovery. Migration Letters, 19(6), 1173–1187. Retrieved from https://migrationletters.com/index.php/ml/article/view/11498

[2] Lekkala, S. (2024). Next-Gen Firewalls: Enhancing Cloud Security with Generative AI. In Journal of Artificial Intelligence & Cloud Computing (Vol. 3, Issue 4, pp. 1–9). Scientific Research and Community Ltd. https://doi.org/10.47363/jaicc/2024(3)404

[3] Manikanth Sarisa , Gagan Kumar Patra , Chandrababu Kuraku , Siddharth Konkimalla , Venkata Nagesh Boddapati. (2024). Stock Market Prediction Through AI: Analyzing Market Trends With Big Data Integration . Migration Letters, 21(4), 1846–1859. Retrieved from https://migrationletters.com/index.php/ml/article/view/11245

[4] Tulasi Naga Subhash Polineni , Kiran Kumar Maguluri , Zakera Yasmeen , Andrew Edward. (2022). AI-Driven Insights Into End-Of-Life Decision-Making: Ethical, Legal, And Clinical Perspectives On Leveraging Machine Learning To Improve Patient Autonomy And Palliative Care Outcomes. Migration Letters, 19(6), 1159–1172. Retrieved from https://migrationletters.com/index.php/ml/article/view/11497

[5] 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

[6] Chandrababu Kuraku, Shravan Kumar Rajaram, Hemanth Kumar Gollangi, Venkata Nagesh Boddapati, Gagan Kumar Patra (2024). Advanced Encryption Techniques in Biometric Payment Systems: A Big Data and AI Perspective. Library Progress International, 44(3), 2447-2458.

[7] 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

[8] 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

[9] Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Janardhana Rao Sunkara, Hemanth Kumar Gollangi (2024) AI-Driven Phishing Email Detection: Leveraging Big Data Analytics for Enhanced Cybersecurity. Library Progress International, 44(3), 7211-7224.

[10] Lekkala, S., Gurijala, P. (2024). Leveraging AI and Machine Learning for Cyber Defense. In: Security and Privacy for Modern Networks. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0823-4_16

[11] Aravind, R. (2024). Integrating Controller Area Network (CAN) with Cloud-Based Data Storage Solutions for Improved Vehicle Diagnostics using AI. Educational

Administration: Theory and Practice, 30(1), 992-1005.

[12] Pandugula, C., Kalisetty, S., & Polineni, T. N. S. (2024). Omni-channel Retail: Leveraging Machine Learning for Personalized Customer Experiences and Transaction Optimization. Utilitas Mathematica, 121, 389-401.

[13] Lekkala, S., Gurijala, P. (2024). Cloud and Virtualization Security Considerations. In: Security and Privacy for Modern Networks. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0823-4_14

[14] Aravind, R., & Shah, C. V. (2024). Innovations in Electronic Control Units: Enhancing Performance and Reliability with AI. International Journal Of Engineering And Computer Science, 13(01).

[15] Lekkala, S., Gurijala, P. (2024). Securing Networks with SDN and SD-WAN. In: Security and Privacy for Modern Networks. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0823-4_12

[16] Madhavaram, C. R., Sunkara, J. R., Kuraku, C., Galla, E. P., & Gollangi, H. K. (2024). The Future of Automotive Manufacturing: Integrating AI, ML, and Generative AI for Next-Gen Automatic Cars. In IMRJR (Vol. 1, Issue 1). Tejass Publishers. https://doi.org/10.17148/imrjr.2024.010103

[17] Aravind, R., Deon, E., & Surabhi, S. N. R. D. (2024). Developing Cost-Effective Solutions For Autonomous Vehicle Software Testing Using Simulated Environments Using AI Techniques. Educational Administration: Theory and Practice, 30(6), 4135-4147.

[18] 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

[19] Aravind, R., & Surabhi, S. N. R. D. (2024). Smart Charging: AI Solutions For Efficient Battery Power Management In Automotive Applications. Educational Administration: Theory and Practice, 30(5), 14257-1467.

[20] Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., Gollangi, H. K. and Rajaram, S. K. (2024) Predictive Analytics for Project Risk Management Using Machine Learning. Journal of Data Analysis and Information Processing, 12, 566-580. doi: 10.4236/jdaip.2024.124030.

[21] Aravind, R. (2023). Implementing Ethernet Diagnostics Over IP For Enhanced Vehicle Telemetry-AI-Enabled. Educational Administration: Theory and Practice, 29(4), 796-809.

[22] Korada, L. (2024). Use Confidential Computing to Secure Your Critical Services in Cloud. Machine Intelligence Research, 18(2), 290-307.

[23] Jana, A. K., & Saha, S. (2024, July). Comparative Performance analysis of Machine Learning Algorithms for stability forecasting in Decentralized Smart Grids with Renewable Energy Sources. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET (pp. 1-7). IEEE.

[24] 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 Artific Intel: JCETAI-101.

[25] Jana, A. K., Saha, S., & Dey, A. DyGAISP: Generative AI-Powered Approach for Intelligent Software Lifecycle Planning.

[26] 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 Artific Intel: JCETAI-102.

[28] Korada, L. (2024). GitHub Copilot: The Disrupting AI Companion Transforming the Developer Role and Application Lifecycle Management. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-365. DOI: doi. org/10.47363/JAICC/2024 (3), 348, 2-4.

[29] Paul, R., & Jana, A. K. Credit Risk Evaluation for Financial Inclusion Using Machine Learning Based Optimization. Available at SSRN 4690773.

[30] 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

[31] Korada, L. (2024). Data Poisoning-What Is It and How It Is Being Addressed by the Leading Gen AI Providers. European Journal of Advances in Engineering and Technology, 11(5), 105-109.

[32] Jana, A. K., & Paul, R. K. (2023, November). xCovNet: A wide deep learning model for CXR-based COVID-19 detection. In Journal of Physics: Conference Series (Vol. 2634, No. 1, p. 012056). IOP Publishing.

[33] 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

[34] Korada, L. Role of Generative AI in the Digital Twin Landscape and How It Accelerates Adoption. J Artif Intell Mach Learn & Data Sci 2024, 2(1), 902-906.

[35] Jana, A. K., & Paul, R. K. (2023, October). Performance Comparison of Advanced Machine Learning Techniques for Electricity Price Forecasting. In 2023 North American Power Symposium (NAPS) (pp. 1-6). IEEE.

[36] 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

[37] Pradhan, S., Nimavat, N., Mangrola, N., Singh, S., Lohani, P., Mandala, G., ... & Singh, S. K. (2024). Guarding Our Guardians: Navigating Adverse Reactions in Healthcare Workers Amid Personal Protective Equipment (PPE) Usage During COVID-19. Cureus, 16(4).

[38] Patra, G. K., Kuraku, C., Konkimalla, S., Boddapati, V. N., & Sarisa, M. (2023). Voice classification in AI: Harnessing machine learning for enhanced speech recognition. Global Research and Development Journals, 8(12), 19–26. https://doi.org/10.70179/grdjev09i110003

[39] Mandala, V., & Mandala, M. S. (2022). ANATOMY OF BIG DATA LAKE HOUSES. NeuroQuantology, 20(9), 6413.

[40] Sunkara, J. R., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., & Gollangi, H. K. (2023). Optimizing Cloud Computing Performance with Advanced DBMS Techniques: A Comparative Study. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication.