Volume 12, No.4, April 2025
Journal of Global Research in Mathematical Archives
RESEARCH PAPER
Available online at http://www.jgrma.info
ISSN 2320 – 5822

Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study

Vikas Prajapati
Independent Researcher
Prajapati.vikas2707@gmail.com

***Abstract*—In a number of industries, including cybersecurity, healthcare, banking, and power distribution, big data analysis has emerged as a game-changing technique. The proliferation of massive and heterogeneous information gathered from platforms, including social media, IoT devices, electronic conducted online, and network logs, necessitates advanced analytical techniques and robust technologies for effective processing and insight generation. This research investigates how statistical analysis of big data may be integrated into cybersecurity, emphasizing its role in anomaly detection, behavioral analysis, threat intelligence integration, and event correlation to enhance threat detection, response, and prediction. Despite its transformative potential, issues including security, confidentiality, effectiveness, and knowledge storage remain significant barriers to its adoption. In order to overcome these obstacles and progress in the sector, emerging technologies like blockchain integration, sophisticated data visualization, and IoT convergence provide encouraging answers. By leveraging these innovations, organizations can improve their ability to anticipate, mitigate, and respond to sophisticated cyber threats, ensuring robust protection for sensitive data and systems.**

***Keywords*—Big Data Analytics, Cybersecurity, Anomaly Detection, Behavioural Analysis, Threat Intelligence, Event Correlation, Blockchain, Data Visualization, IoT Integration, Data Privacy.**

I. INTRODUCTION

The numerous industries and disciplines, including those in power distribution of wealth, healthcare, psychology, insurance coverage, and financial markets, as well as public organizations, have started to use big data analysis [1]. The importance of large-scale data assessment has increased in both modern industry and research. Online operations, emails, videos, music, images, click streams, logs, posts, enquiries about searches, medical information, social networking relationships, sensors, portable devices, scientific data, and the applications that run on them all generate this type of data. Storage, administration, sharing, analysis, and data visualization are all difficult activities that call for sophisticated programs and database tools since big data is kept in platforms that expand gradually and hold a lot of information [2]. The volume of data in several fields has significantly increased during the past 20 years.

In the period of prevalent replicated intimidations [3], Organizations, buyers, and policymakers are becoming very concerned about how cyber-security disasters affect ethical behavior and company values [4]. Instances involving cybercrime highlight the harm to one's standing, changes in shareholder opinion, and pecuniary consequences that may arise from these intrusions [5]. Therefore, it is possible to consider cybercrime happenings as a risk of social responsibility for business non-compliance. Their goal is to quantify the risk component of societal accountability that might arise from cybersecurity events [6].

In this context, improving real-time threat identification and response has been substantially facilitated by incorporating big data analytics and ML into cybersecurity frameworks. ML algorithms can swiftly examine large data sets and identify patterns and anomalies that may indicate potential cyber threats. When combined with big data analytics, these technologies enable continuous monitoring and real-time network traffic analysis [7]. System logs and user behavior enable the quick identification and elimination of threats before they have a chance to do serious damage.

Big Data's role in protection is more important than ever at a time when powerful espionage tactics, computer hacking, and data breaches are becoming more common and serious [8]. An organization can discover and react to threats instantly, see trends and abnormalities that point to fraudulent activity, and anticipate future assaults before they happen when Big Data research is integrated into protection [9]. Security professionals can review information obtained from social media, threat intelligence streams, and other sources, user activity, and network logs to obtain a complete picture of their protected environment [10], enabling companies to successfully detect weaknesses, keep an eye on possible threats, and reduce risks [11]. Sophisticated threat identification and avoidance are two areas where big data analytics is very useful

A. Structure of the Study

This paper is structured as follows: A summary of big data is given in Section II, emphasizing its features and importance. Big data analytics' application in cybersecurity is examined in Section III, with an emphasis on how it improves threat detection and response systems. Section IV, real-world applications, implementation strategies, and security measures that incorporate big data analytics. Section V examines emerging trends and Big Data analytics problems for cybersecurity while talking about advancements, limitations, and potential risks. A review of the literature is given. in Section VI, which examines current studies and approaches in the area. Section VII wraps up the study by outlining the main conclusions, going over the limitations, and offering ideas for future research possibilities.

II. Overview of Big Data

The term "big data" refers to a rapidly growing collection of enormous and varied data in both organized and unorganized formats [12] and forms that are unstructured. Big data's complexity necessitates the use of powerful technology, sophisticated algorithms, and conventional commercial resources for administration and interpretation are ineffective at handling large amounts of data.

A. Definition of Big Data Analytics

The technology of the collection makes up the foundation of BD analytics [13], Tools and methods for mining information analytics approaches and strategies that businesses may use to examine large volumes of intricate data for a range of applications designed to improve business performance from several angles. BD may be seen as an operation as well as a person or thing [14]. The whole of BD is made up of semi-structured as well as structured information that has been collected from a range of sources both inside and outside the organization [15] and unorganized information that conventional databases and software methods are unable to handle. As a process, BD encompasses the technology and organizational infrastructures employed to gather, preserve, and examine different types of data [16].

B. Characteristics of Big Data

Three key features are used by the majority of the "3Vs" by data scientists and big data experts to describe huge data, shown in Figure 1.

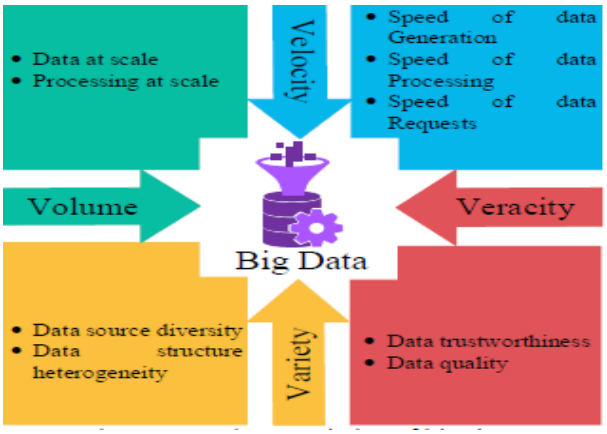

Fig. 1. Characteristics of Big Data

- **Volume:** The course of time, the amount of data that complies with the big data standard grows and changes continuously. Big Data contains a lot of data that ranges in size from terabytes to zettabytes [17].
- **Velocity:** The amount of data depends on the rate at which it is generated, which necessitates quick processing of the data to glean insightful information. The term "velocity" describes the instantaneous nature of big data, and its potential advantages for organizations must be maximized by timely and effective data collection, analysis, and deployment [18].
- **Variety:** Data may be classified as partially structured (like XML data), hierarchical (like database data), or unregulated (like sound, photos, videos, websites, text, etc.).

III. Role Of Big Data Analytics In Cybersecurity

A. Overview of Cybersecurity

The technique of defending systems linked to the internet, including information, applications, and equipment, from security breaches is known as a cyberattack [19]. People and businesses use it to prevent unwanted utilization of data centers alongside other computerized systems.

A robust security posture against malevolent assaults intended to acquire access may be provided by an efficient counterterrorism strategy [20], change, remove, annihilate, or extort highly confidential information and systems belonging to a user or an organization [21]. Additionally, cybercrime plays a key role in thwarting assaults intended to interfere with or deactivate the functionality of a system or device.

B. Big Data Analytics in Cybersecurity

Originating from the fields of technical advancement and large data collecting [22], protection of data, systems, networks, and information against unauthorized access, theft, and destruction of a nation or an organization is the main goal of the crucial field of cybersecurity study and implementation. "Big data" refers to massively aggregated object-oriented data, and big data analytics provides the greatest solutions for managing, organizing, and mining this type of data [23]. In addition to anticipating, sensing, and responding to the vast amount of privacy and security data, big statistical analysis may assist in risk decision-making and the identification of possible business problems [24].

A combination of the introduction of big data statistical analysis, cybercrime has advanced dramatically, transforming how businesses safeguard their data networks, including systems information to find possible dangers and weaknesses [25].

IV. Application Of Big Data Analytics In Cybersecurity

There are several applications for big data analytics in cybersecurity, including this-

A. Anomaly Detection

In order to identify irregularities that may indicate a cyberattack, algorithms for big data analytics could examine data on user activities, system logs, and network traffic. Security problems may be detected more rapidly if businesses establish baseline behavior patterns and monitor for variations from these patterns [26][27].

B. Cyberattack Trends and Pattern Recognition

ML, data mining, and other big data analytics tools can identify trends and patterns in cyberattack strategies and tactics [28][29]. By reviewing attack data from the past and looking for trends, businesses might become more adept at anticipating and addressing cyberattacks.

C. Behavioral Analysis

With the usage of BDA, businesses may examine user actions and spot suspicious patterns, such as attempts at illegal access, data exfiltration, or privilege escalation. Company insider threats and compromised accounts may be detected by tracking user activity across many platforms and apps.

D. Integrating Threat Intelligence

In order to discover new vulnerabilities and threats, BDA systems may take in and process information from several resources, including threat intelligence feeds and the dark web. Organizations may proactively protect and cover themselves against cyber assaults by comparing internal security data with external threat information in order to detect signs of penetration[30]

E. Event Correlation:

In order to discover possible security problems [31], big data analytics technologies may correlate security alerts and events from several sources [32], including Security for endpoints remedies, network firewalls, and detection systems for intrusions [18]. Organizations may improve response effort prioritization and decrease false positives by combining and correlating data from several sources.

V. Emerging Trends And Challenges In Big Data Analytics For Cybersecurity

A. Emerging Trends

These are a few developments in cybersecurity Big Data Analytics:

1) Blockchain Integration

Blockchain technology and massive amounts of data have evolved gradually with human civilization [34]. Despite the advancement of big data technologies, issues data leakage, data silos, and inaccurate data are still problems, and big data risk management isn't perfect. Blockchain is based on three main principles: decentralization, transparency, and availability [35]. By addressing the issue of online trust, cryptocurrencies can support the growth of big data and the digital economy.

2) Advanced Data Visualization and Reporting

It seems that data visualization is a graphical depiction of the data [36]. To assess, it is necessary to understand data visualization and gain deeper insights from large amounts of data. Data visualization aids in understanding data interactions and connecting disparate data pieces [37], Real-time discussion of problems and quick decision-making on the areas of your inquiry [38].

3) Integration of IoT

IoT has been quickly expanding across several sectors [39]. The IoT is made up of gadgets that gather data and use it to establish connections with the outside world. It may utilize this data to solve a variety of research problems in one way or another. Numerous big data analysis methods and approaches may be useful in the analysis of all of this information. In this view, Big Data and the IoT are complementary concepts [40].

B. Challenges

The following are some of the difficulties in applying big data analytics to cybersecurity:-

1) Data Storage

A large and complex system of interconnected computer networks is required to collect, store, and process enormous volumes of personally identifiable information that is fundamental to the operation of a company. The importance of storage solutions for information is growing due to the constantly growing amount of data, and to maintain competitiveness, many cloud organizations strive for massive storage capabilities.

2) Data Quality

Information timeliness and preciseness are cornerstones of decision-making. Having a metadata management method to guarantee data quality is essential for big data to be valuable.

3) Security and Privacy

The need to maintain privacy is one of the most difficult problems with large data. By combining some of their sensitive data with the larger data sets, companies may better understand big data [41]. A major issue with huge data is confidentiality. To gain a deeper understanding of big data, organizations should begin incorporating some of their private information into the broader dataset [42], simultaneously making certain that data analytics are maximized and unhindered by such regulations.

VI. Security And Privacy

The following section provides the study of the literature on how big data analytics might enhance information security and threat detection.

Ge and Xu (2020) In this study, individuals focus more on the Information ionization background for Technology for protecting computer networks and associated safeguards. An introduction to informatization is given at the beginning of this article, and the topic of information security management systems for computer networks is then covered. Next, specific information technology applications and problems in computer network security management systems are examined, including the use of computer network assurance protection systems in information settings and the protection of information networks through hash functions, and the defense of machine network information security using asymmetrical encryption [43].

Cuzzocrea (2021) according to According to this study, big data lakes follow logically from data warehouse solutions in the big data environment and satisfy a range of requirements brought forth by big data's well-known 3V nature. As the vast data lake research effort expanded, more issues emerged, including Models for big data lakes, frameworks for big data lakes, and methods for big data lakes. This article offers an overview of innovative open issues and themes that guide future research directions, as well as cutting-edge approaches that serve as the field's cornerstone, in order to further the big data lake research trend [44].

Singh et al. (2022) offer a thorough, in-depth analysis of the big data industry. There are many different sources of big data, and the term was created as a result of the quick uptake of technology advancements. Three goals are addressed in the paper's discussion of the big data landscape: First, to showcase recent advancements and features in the infrastructure for big data and big information analysis; second, to talk about the big data platform designing principles as well as its tools and methods, but and in third place to present the key challenges when technical concerns in the core idea behind big data. In recent years, there has been a considerable growth in the quantity of data that can be gathered and used [45].

Alawadhi et al. (2024) explore how Big Data might improve cybersecurity protocols, emphasizing the critical function of BDCA systems. The article specifically examines the fundamental obstacles that the cybersecurity field must

overcome and how Big Data ideas and techniques might be used to solve these problems. The study highlights the ethical and privacy ramifications while assessing the potential and inherent difficulties of using big data in cybersecurity. Additionally, there are recommendations for the wise and effective application of big data in cybersecurity, highlighting the necessity of finding a balance between information security and development [46].

Liu (2022) presents a big data-based approach to managing computer network information security. To acquire network traffic information, install the network probe on the PC server. The characteristic index of the internet traffic information will be chosen using the tabu search method and the analysis of the principal components. Based on BP neural network categorization and abnormal behavior recognition, unlawful attacks may be stopped early, and network information security can be guaranteed. The design technique has an excellent security management impact, as shown by the testing findings, which indicate that the detection rate of the four attack mechanisms is above 95% and the false positive rate is less than 1.5% [47].

Khan et al. (2023) The purpose of this endeavor is to classify cyber threat intelligence for businesses. Although it is often disregarded, cyber threat intelligence is a crucial part of a cybersecurity operation. It may help detect possible upcoming cyber threats. Large amounts of data that include cyber threat intelligence are processed by organizations. However, this data can frequently not be gathered, approved, or regarded as cyber intelligence about threats. If nothing is done, South African organizations will continue to suffer from cyberattacks [48].

Naseer and Siddiqui (2022) make the case that businesses should increase the agility of their incident response process in order to respond to cybersecurity assaults. This technique heavily relies on big data analytics. Their framework, which is based on 21 in-depth expert interviews, outlines the primary characteristics and outcomes of big data analytics in the course of accident response at three distinct levels: manual, advanced, and basic analysis. By using big data analytics at higher levels of analysis, the incident response process gains the agile qualities of speed, inventiveness, and adaptability [49].

Table I examines network security, information security, and big data, emphasizing issues including intelligence about threats, data management, and privacy. Agile incident response, AI-based security models, and big data integration for improved cybersecurity and information-driven network security administration are some of the major contributions.

TABLE I. COMPARATIVE ANALYSIS OF STUDY ON BIG DATA ANALYTICS IN CYBER SECURITY AND THREAT DETECTION

Reference	Focus Area	Key Findings	Challenges	Key Contribution
Ge and Xu (2020)	Computer Network Security and Informatization	Informatization enhances network security through hash functions, symmetric encryption, and security protection systems.	Ensuring effective implementation of security measures in informatization.	Provides insights into informatization in network security management.
Cuzzocrea (2021)	Big Data Lakes	Overview of huge data lake frameworks, concepts, and methods. draws attention to research gaps and potential directions.	Challenges in handling large-scale data storage, processing, and management.	Identifies key issues in big data lakes and suggests research advancements.
Singh et al. (2022)	Analytics & Big Data Landscape	Reviews big data characteristics, system design, tools, and techniques. discusses the difficulties of managing enormous amounts of data.	Managing the increasing complexity of big data systems.	provides a comprehensive analysis of big data analytics.
Alawadhi et al. (2024)	Big Data-Based Cybersecurity	Examines the opportunities and challenges of cybersecurity utilizing big data. tackles ethical and privacy concerns.	Balancing innovation with data protection and privacy.	Suggests integrating big data in cybersecurity in a responsible manner.
Liu (2022)	Network Security and Big Data	Proposes a network security method using big data analytics with BP neural networks. Achieves high attack detection rates.	Ensuring the adaptability and efficiency of AI-based security models.	Develop an effective anomaly detection approach for network security.
Khan et al. (2023)	Information about Cyberthreats	Highlights the significance of cybersecurity's use of Cyber Threat Intelligence (CTI). finds gaps in the implementation of CTI.	Lack of structured CTI utilization in organizations.	Emphasizes the need for better CTI collection and processing.
Naseer and Siddiqui (2022)	Response to Incidents and Analytics of Big Data	Leverages big data analytics to develop an adaptable incident response system.	Challenges in scaling big data analytics for incident response.	offers an organized method for improving cybersecurity incident response.

VII. CONCLUSION AND FUTURE WORK

Big Data Analytics is becoming an essential component of contemporary cybersecurity, allowing companies to identify, evaluate, and handle risks with previously unheard-of efficiency. Cybersecurity experts can analyze enormous volumes of structured and unstructured data to spot irregularities, anticipate possible attacks, and improve overall threat management tactics by using Big data's three Vs: variety, velocity, and volume. Notwithstanding its benefits, the sector has drawbacks, such as restrictions on data storage, maintaining data quality, and handling privacy and security issues. These challenges highlight the need for strong regulations, expandable infrastructure, and creative methods to maximize Big data applications in cybersecurity.

Future studies ought to concentrate on applying big data analytics to improve data security, transparency, and compatibility with emerging technologies like blockchain and the IoT. Furthermore, developments in ML and AI may improve predictive capacities even further, allowing for real-time reactions to changing cyber threats. In order to ensure regulatory compliance and enable smooth data exchange, efforts should also be focused on creating standardized frameworks for data privacy and security. Addressing these areas will pave the way for more resilient cybersecurity

systems, capable of safeguarding sensitive information in an increasingly interconnected digital landscape.

REFERENCES

[1] M. Mahmoudian, S. M. Zanjani, H. Shahinzadeh, Y. Kabalci, E. Kabalci, and F. Ebrahimi, "An Overview of Big Data Concepts, Methods, and Analytics: Challenges, Issues, and Opportunities," in *2023 5th Global Power, Energy and Communication Conference (GPECOM)*, IEEE, Jun. 2023, pp. 554–559. doi: 10.1109/GPECOM58364.2023.10175760.

[2] S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," *Int. J. Multidiscip. Res.*, vol. 3, no. 4, pp. 1–10, 2021.

[3] Suhag Pandya, "Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 865–876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.

[4] S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure : Ensuring Compliance and Security in Utility Systems," *Int. J. Innov. Res. Creat. Technol.*, vol. 8, no. 2, pp. 1–8, 2022.

[5] W. Khan, J. Lee, and S. Liu, "Is Cybersecurity a Social Responsibility?," *Inf. Syst. Front.*, pp. 1–25, 2025, doi: 10.1007/s10796-024-10565-z.

[6] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: https://jgrec.info/index.php/jgrec.

[7] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," *Comput. Sci. IT Res. J.*, vol. 4, no. 3, pp. 478–501, 2023, doi: 10.51594/csitrj.v4i3.1500.

[8] M. Gopalsamy and K. B. Dastageer, "The Role of Ethical Hacking and AI in Proactive Cyber Defense : Current Approaches and Future Perspectives," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, 2025, doi: https://doi.org/10.5281/zenodo.14916984.

[9] J. Brandon and E. Edward, "Big Data Analytics in Cybersecurity: Enhancing Threat Detection, Response, and Prediction," *Int. J. Adv. Eng. Technol. Innov.*, vol. 6, no. 2, 2024.

[10] A. Goyal, "Optimising Cloud-Based CI/CD Pipelines: Techniques for Rapid Software Deployment," *Tech. Int. J. Eng. Res.*, vol. 11, no. 11, pp. 896–904, 2024.

[11] J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–879, 2021.

[12] H. Shahinzadeh, s. M. Zanjani, J. Moradi, M.-H. Fayaz-Dastgerdi, W. Yaïci, and M. Benbouzid, "The Transition Toward Merging Big Data Analytics, IoT, and Artificial Intelligence with Blockchain in Transactive Energy Markets," 2022. doi: 10.1109/GEC55014.2022.9986604.

[13] Z. A. Al-Sai, R. Abdullah, and M. H. Husin, "Big Data Impacts and Challenges: A Review," *2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc.*, no. April, pp. 150–155, 2019, doi: 10.1109/JEEIT.2019.8717484.

[14] S. R. Thota, S. Arora, and S. Gupta, "Hybrid Machine Learning Models for Predictive Maintenance in Cloud-Based Infrastructure for SaaS Applications," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, IEEE, Jul. 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691295.

[15] A. Gogineni, "Artificial intelligence-Driven Fault Tolerance Mechanisms for Distributed Systems Using Deep Learning Model," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 4, 2023.

[16] Godavari Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 1, no. 12, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.

[17] A. Gogineni, "Advancing Kubernetes Network Stack for High-Performance AI/ML Workloads," *Int. J. Sci. Technol.*, vol. 15, no. 4, 2024.

[18] S. M. Zanjani, S. M. Hasan Zanjani, H. Shahinzadeh, Z. Rezaei, B. Kaviani-Baghbaderani, and J. Moradi, "Big Data Analytics in IoT with the Approach of Storage and Processing in Blockchain," in *2022 6th Iranian Conference on Advances in Enterprise Architecture (ICAEA)*, IEEE, Nov. 2022, pp. 1–6. doi: 10.1109/ICAEA57644.2022.10054018.

[19] M. Shah, P. Shah, and S. Patil, "Secure and Efficient Fraud Detection Using Federated Learning and Distributed Search Databases," in *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, 2025, pp. 1–6. doi: 10.1109/ICAIC63015.2025.10849280.

[20] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security : Challenges and Solutions," pp. 6–18, 2025, doi: 10.48175/IJARSCT-23902.

[21] A. R. A. K. Muhammad Ismaeel Khan, Aftab Arif, "The Most Recent Advances and Uses of AI in Cybersecurity," *BULLET*, vol. 3, no. 4, pp. 566–578, 2024.

[22] S. Bauskar, C. Madhavaram, E. P. Galla, J. R. Sunkara, and H. K. Gollangi, "AI-Driven Phishing Email Detection: Leveraging Big Data Analytics for Enhanced Cybersecurity," *Libr. Prog. Int.*, vol. 44, no. 3, pp. 7211–7224, 2024, doi: http://dx.doi.org/10.56726/IRJMETS41519.

[23] A. V. Hazarika and M. Shah, "Distributed Quantum Computing Models: Study of Architectures and Models for the Distribution of Quantum Computing Tasks Across Multiple Quantum Nodes," *Int. J. Sci. Res. Arch.*, vol. 13, no. 2, pp. 3719–3723, Dec. 2024, doi: 10.30574/ijsra.2024.13.2.2602.

[24] V. Pillai, "Integrating AI-Driven Techniques in Big Data Analytics: Enhancing Decision-Making in Financial Markets," *Int. J. Eng. Comput. Sci.*, vol. 12, no. 7, 2023.

[25] A. K. Aftab Arif, Muhammad Ismaeel Khan, "An overview of cyber threats generated by AI," *Int. J. Multidiscip. Sci. Arts*, vol. 3, no. 4, pp. 67–76, 2024.

[26] M. M. Srinivas Murri, Manoj Bhoyar, Guru Prasad Selvarajan, "Transforming Decision-Making with Big Data Analytics: Advanced Approaches to Real-Time Insights, Predictive Modeling, and Scalable Data Integration," *Int. J. Commun. Networks Inf. Secur.*, vol. 16, no. 5, pp. 506–519., 2024.

[27] P. Piyush, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," *J. Intell. Syst. Internet Things*, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.

[28] A. V. Hazarika and M. Shah, "Exploring Fault Tolerance Strategies In Big Data Infrastructures And Their Impact On Processing Efficiency," *SSRN Electron. J.*, vol. 16, no. 6, pp. 35–40, 2025, doi: 10.2139/ssrn.5078913.

[29] M. Shah and S. Patil, "AI/ML Techniques for Real-Time Fraud Detection," *DZone*, 2025.

[30] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, p. 5, 2023.

[31] P. Agrawal and S. Gandhi, "Big Data Cyber Security Analytics," in *Advanced Cyber Security Techniques for Data, Blockchain, IoT, and Network Protection*, 1st ed., IGI Global, 2024, pp. 21–48. doi: 10.4018/979-8-3693-9225-6.ch002.

[32] S. Murri, "Data Security Challenges and Solutions in Big Data Cloud Environments," *Int. J. Curr. Eng. Technol.*, vol. 14, no. 06, pp. 565–574, Dec. 2024, doi: 10.14741/ijcet/v.12.6.11.

[33] K. Rajchandar, M. Ramesh, A. Tyagi, S. Prabhu, D. S. Babu, and A. Roniboss, "Edge Computing in Network-based Systems: Enhancing Latency-Sensitive Applications," in *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, 2024, pp. 462–467. doi: 10.1109/IC3I61595.2024.10828607.

[34] H. Taherdoost, N. Moosavi, N. Mohamed, and I. U. Khan, "Applying Blockchain Technology into Big Data: Advantages and Challenges," *Procedia Comput. Sci.*, vol. 237, pp. 827–832, 2024, doi: https://doi.org/10.1016/j.procs.2024.05.171.

[35] P. Piyush, N. S. Gill, P. Gulia, D. D. Rao, Y. Mandiga, and P. K. Pareek, "Systematic Analysis of threats, Machine Learning solutions and Challenges for Securing IoT environment," *J. Cybersecurity Inf. Manag.*, vol. 14, no. 2, pp. 367–382, 2024, doi: 10.54216/JCIM.140227.

[36] Z. Khalid and S. Zeebaree, "Big Data Analysis for Data Visualization: A Review," *Int. J. Sci. Bus.*, vol. 5, no. 2, pp. 64–75, 2021, doi: 10.5281/zenodo.4462042.

[37] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, 2021, doi: DOI: 10.48175/IJARSCT-6268B.

[38] A. Arif, A. R. A. Khan, and M. I. Khan, "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review," *JURIHUM J. Inov. dan Hum.*, vol. 2, no. 3, pp. 297–311, 2024.

[39] Soni Kumari and Dona Chakraborty, "A Review on Big Data Analytics and Its Tools," *Int. J. Sci. Res. Sci. Technol.*, vol. 11, pp. 414–417, Dec. 2023, doi: 10.32628/IJSRST52310684.

[40] V. Pillai, "Techniques for Processing and Analyzing Large Data Sets Using Big Data Analytics," *J. Emerg. Technol. Innov. Res.*, vol. 11, no. 10, 2024.

[41] A. Gogineni, "Chaos Engineering in the Cloud-Native Era: Evaluating Distributed AI Model Resilience on Kubernetes," *J Artif Intell Mach Learn Data Sci 2024*, vol. 3, no. 1, pp. 2182–2187, 2025.

[42] B. M. Balachandran and S. Prasad, "Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence," in *Procedia Computer Science*, 2017. doi: 10.1016/j.procs.2017.08.138.

[43] B. Ge and J. Xu, "Analysis of Computer Network Security Technology and Preventive Measures under the Information Environment," in *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, 2020, pp. 1978–1981. doi: 10.1109/ICMCCE51767.2020.00433.

[44] A. Cuzzocrea, "Big data lakes: Models, frameworks, and techniques," in *Proceedings - 2021 IEEE International Conference on Big Data and Smart Computing, BigComp 2021*, 2021. doi: 10.1109/BigComp51126.2021.00010.

[45] J. Singh, G. Singh, and A. Verma, "The Anatomy of Big Data: Concepts, Principles and Challenges," in *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2022, pp. 986–990. doi: 10.1109/ICACCS54159.2022.9785082.

[46] R. Alawadhi, H. Aalmohamed, S. Alhashemi, and H. A. Alkhazaleh, "Application of Big Data in Cybersecurity," in *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, 2024, pp. 1–6. doi: 10.1109/ICSPIS63676.2024.10812589.

[47] Z. Liu, "Research on computer network information security management and protection strategy," in *2022 International Conference on Computers, Information Processing and Advanced Education (CIPAE)*, 2022, pp. 200–203. doi: 10.1109/CIPAE55637.2022.00050.

[48] Z. C. Khan, T. Mkhwanazi, and M. Masango, "A Model for Cyber Threat Intelligence for Organisations," in *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, 2023, pp. 1–7. doi: 10.1109/icABCD59051.2023.10220503.

[49] A. Naseer and A. M. Siddiqui, "The Effect of Big Data Analytics in Enhancing Agility in Cybersecurity Incident Response," in *2022 16th International Conference on Open Source Systems and Technologies (ICOSST)*, 2022, pp. 1–8. doi: 10.1109/ICOSST57195.2022.10016853.

