Grenze International Journal of Engineering and Technology, January Issue

Harnessing Big data Analytics for Proactive Cyber Threat Intelligence in Health care Information System

Vinesh K V[1] and Dr. Abhishek Tripathi[2]
[1-2]Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnanakoil, Virudhunagar Dt., Tamil Nadu, India-626126
Email: vineshvpai@gmail.com, tripathi.abhishek.5@gmail.com

***Abstract*— Healthcare organizations are presented with historic cybersecurity challenges as they continue to digitize patient data and medical equipment, producing enormous sets of sensitive information that are sought after by malicious intent. This research explores the potential for the application of big data analytics methods to improve cyber security threat intelligence functions within healthcare database environments. Through the use of machine learning algorithms, real-time data processing, Apache HDFS, Spark and sophisticated pattern recognition techniques, we can create a broad framework for detecting, analysing and counteracting cyber threats to healthcare information systems and databases. The research project has a multi-layered solution that makes use of network traffic analysis, user behaviour analytics, and anomaly detection algorithms to analyse volumes of security logs, audit trails, and system metadata within a large healthcare database infrastructure. The framework proposed here combines structured and unstructured data sources such as firewall logs, intrusion detection system notifications, authentication records, and threat intelligence feeds to provide a comprehensive threat landscape view.**

The application of predictive analytics models fortified proactive threat hunting ability, enabling security professionals to foretell and avert likely attacks prior to their occurrence. Our research demonstrates that big data analytics could revolutionize healthcare cybersecurity from reactive to predictive, seriously enhancing protection of sensitive patient data and guaranteeing conformity with healthcare data safeguarding regulations like DPDP and IT Act2000. This study adds to the increasing repository of healthcare cybersecurity knowledge and offers an actionable model for organizations that want to exploit big data technologies to achieve better threat intelligence and safeguarding of critical healthcare infrastructure.

***Keywords*— Big Data Analytics, Cyber Threat Intelligence, Healthcare Information System, Patient Health Information Proactive Intrusion Detection.**

I. INTRODUCTION

Big data and cyber security are now mainstream. For the majority of firms, this entails opportunity as well as risk. Big data, which is the term used to describe a very huge data set that is mined and examined to uncover patterns and behavioural trends, is probably something you are quite familiar with if you work in the cyber security industry. It is typically described as dense in volume, pace, and diversity. Big data has opened up new opportunities for analytics and security solutions to safeguard data and fend off future cyberattacks from the perspective of cyber security.

Grenze ID: 01.GIJET.12.1.366

But just as big data has given cyber security teams new options, it has also made it possible for hackers to acquire enormous volumes of private and sensitive data by utilising cutting-edge technologies. Big data refers to the usage of significant amounts of data that are too complex or heavy for conventional methods. Companies handle, process, and analyse that data in order to monitor trends and obtain insights into how to better certain parts of a business, like operations. Generally speaking, larger data sets yield larger insights. To completely comprehend the vast amount of data and then analyse and interpret it in a way that will boost business performance, many firms have had difficulty. To make the greatest decisions for your company, you must perform accurate data analysis. Collected cancer patient records can be further processed for clinical insights, early diagnosis, and personalized treatment prediction. Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks, theft, or damage. It involves a combination of technologies, processes, and practices designed to safeguard digital assets and ensure the confidentiality, integrity, and availability of information. Cyber threats typically arise when an individual or organization's data, computer system, network, or device is targeted by a cyber attacker who seeks to gain unauthorized access or exploit any vulnerabilities present in the information system, compromising its confidentiality, integrity, or availability.

A. History of Healthcare databases.

Healthcare organizations face unique cybersecurity challenges due to the high value of protected health information (PHI) and the critical nature of healthcare services. Big data analytics provides powerful capabilities to enhance threat intelligence by processing vast amounts of security data to identify, predict, and respond to cyber threats more effectively. Healthcare databases store highly sensitive and valuable information, making them prime targets for various cyber threats. Different types of threats exist in real time system. Here, this project deals only with Denial of Service (DoS) attack.

A Denial of Service (DoS) attack on healthcare information systems is a cyberattack designed to disrupt the availability of critical medical services and data by overwhelming system resources or exploiting vulnerabilities to render systems unusable.

DoS (Denial of Service): An attacker floods a server with traffic or requests to overwhelm it and cause service failure.

DDoS (Distributed Denial of Service): A large-scale version of DoS using multiple compromised systems (botnets) to generate traffic.

B. Impact on Healthcare Information Systems

TABLE I

Area Affected	Effect of DoS/DDoS Attack
Electronic Health Records (EHR)	Doctors and nurses cannot access patient histories or diagnostic data.
Appointment Systems	Patients can't book, reschedule, or check appointments.
Emergency Services	Ambulance dispatch and triage systems may go offline, delaying critical care.
Billing and Insurance	Financial processing halts; insurance claims delayed or lost.
Medical Devices & IoT	Connected equipment (e.g., monitors, infusion pumps) may lose data sync or control.
Patient Portals	Patients may lose access to personal health data.

C. Safeguarding Cancer patients - Information System

Healthcare information systems, particularly those dealing with pathology data of cancer patients, are valuable targets owing to the privacy and quantity of personal as well as clinical information they contain. Digitization of health records and laboratory data in India has accelerated at a faster pace than security, making vulnerabilities more exposed. Big data analytics can be a powerful aid by consuming huge amounts of heterogeneous security and usage data to identify early threats. Healthcare has emerged as the most targeted industry in India. Industry reports indicate 22 % of all cyberattacks in India aim at healthcare, surpassing all other industries. A 2024 India Cyber Threat Report highlighted that hospitals and clinics are particularly vulnerable: they possess sensitive personal/medical information and operate mission-critical systems (e.g. radiation therapy devices, laboratory analysers) that can't be readily taken offline. Thieves take advantage of these factors, usually spreading ransomware or silent malware. Indian hospital groups averaged more than 8,600 weekly cyberattacks in the first half of 2024.

High-profile breaches demonstrate the risk. In April 2024, the Thiruvananthapuram Regional Cancer Centre (RCC) – Kerala's public sector cancer hospital – was hit by a catastrophic cyberattack. Eleven of its servers were compromised, and systems for radiation therapy and pathology reports were hacked. Confidential information on more than 20 lakh Cancer patients – including surgery, radiation and pathology findings were extracted and

attackers demanded a 100 Crores ransom. The attack stopped patient treatment, endangering mistreated patients, and revealed millions of names, addresses, and medical records. The RCC's investigation determined that it depended on only standard perimeter defences and did not have a policy of layered security. This incident painfully illustrates that without superior analytics and security measures, an attack on pathology data can have life-threatening and systemic consequences.

Cancer pathology information is particularly sensitive. It contains extensive medical histories, laboratory test results, genomic sequences, and images used for diagnosis – all of which disclose individual health information. Such information tends to remain in systems for numerous years, increasing exposure risk. In the case of patients, confidentiality violations (e.g. unveiling of a cancer diagnosis) may lead to social stigmatization or discrimination. For organizations, pathology labs can harbour intellectual property research (e.g., new biomarkers) that may be hacked or sold by attackers. Pathology labs in India can vary from big public research institutions to small private labs but all store personally identifiable information (PII) in addition to diagnostic test results.

Cybersecurity processes vary widely between India's private and public healthcare. Government cancer centres (such as the RCC) and public hospitals frequently have restricted budgets. They might use old systems and possess few specialized IT security personnel. The RCC example revealed just perimeter security with an entry level Unified Threat Management and no multi-layered defence. Large private hospitals and chains, on the other hand, are spending liberally on cybersecurity. Business Standard recently noted top hospital chains spending 8–10% of IT budgets on cybersecurity, from 4–7% spent in 2021, to reach 12–15% by 2027.

D. Tools and Technologies needed for the Research project.

- Apache MongoDB // for flexible healthcare data models, handling unstructured threat intelligence data.
- Machine Learning Algorithm // to enhance threat intelligence.
- Apache Hadoop Distributed File System (HDFS) // for storing large volumes of healthcare security logs and threat data.
- Apache Spark // for real-time and batch processing, for distributed data processing and analytics.
- Apache Spark Mllib // for machine learning on large datasets, for distributed machine learning on security data.

II. Research Methodology

A. Big Data Analytics Applications in Cyber Security.

Big data analytics; is a process of analysing large and diverse datasets to discover hidden patterns, relationships, market trends, and customer behaviour, eventually assisting organizations in making more intelligent business decisions. It is a process of utilizing specialized techniques and tools to obtain meaningful insights from huge amounts of structured, semi-structured, and unstructured data. Refer the pointers below to learn about big data analytics. This research project can effectively be utilized for both cybersecurity (DoS detection) and clinical outcomes (Cancer data analysis), can build a dual-purpose big data architecture as follows. Collected cancer patient records can be further processed for clinical insights, early diagnosis, and personalized treatment prediction.

Fig 1: Big Data Analytics in Cyber Security

The above figure shows the different environments of utilizing big data analytics in cyber security. This research title deals with cyber threat intelligence and clinical outcomes (Cancer data analysis), can build a dual-purpose

big data architecture as follows. Collected cancer patient records can be further processed for clinical insights, early diagnosis, and personalized treatment prediction. The following pointers indicates different big data analytics strategies.

B. Statistical techniques detecting potential frauds

Fraud detection can be generally improved with big data analytics. Certain statistical methods employed in data analysis involve error detection, verification, correction, and gap filling due to erroneous or missing data.

C. Effortless anomaly detection algorithms

Conventional models, firewalls, and threat detection software were basically outdated in the manner they responded to intrusion, hence rendering them powerless against modern-day cybersecurity attacks. Big data analytics have found their way into cyber security networks such that cyber defence engineers and data scientists are able to correlate algorithms for anomaly detection in the transaction and user activity.

Big data analytics strengthens cyber security networks by the above-mentioned method, and also helps reduce false alarm rates, estimate potential threats, and predict the future. Cyber defence management has never been an easy task that needs a great deal of knowledge and a considerable amount of time. The comparatively fast-growing depth of big data analytics has significantly improved the time required to cross-correlate data for purposes of forensics and create meaningful security solutions.

D. Computation of Statistical Parameters

Big data analytics can rapidly compute a vast array of statistical parameters, including means, quintiles, performance metrics, and probability distributions.

E. Clustering and classification are made simpler

Data scientists and cyber security professionals can easily cluster and categorise patterns and relationships between huge sets of data using big data analytics. Applying big data analytics to cybersecurity threat intelligence means using enormous amounts of structured and unstructured data for identifying, anticipating, and reacting to threats in an effective manner. Below steps will elaborate on the project work flow.

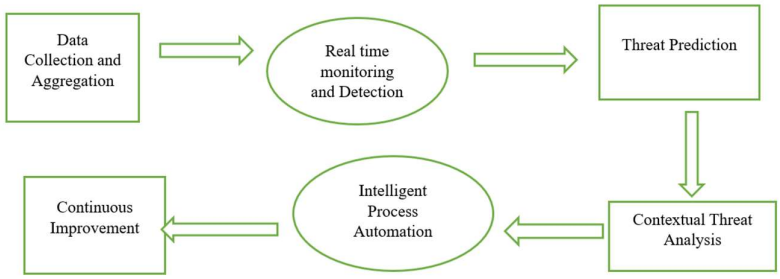

Fig 2: Project Work flow

F. Data Collection and Aggregation

Data Sources: Gather data from various sources like network logs, user behaviour analytics, intrusion detection systems, threat feeds, social media, and dark web intelligence.

Data Storage: Store data on scalable platforms like Hadoop or cloud-based systems for handling large volumes of data.

Normalization: Normalize data coming in various formats to maintain consistency and ease of analysis.

G. Real-Time Monitoring and Detection

Streaming Analytics: Use tools such as Apache Kafka or Spark Streaming to analyse data in real time and identify anomalies.

Machine Learning Models: Apply supervised and unsupervised learning to discover deviation from normal behaviour, meaning potential attacks.

Correlation Analysis: Correlate data points between logs, activities, and sources to find unusual patterns.

H. Threat Prediction

Behavioural Analytics: Use past data to forecast future attack vectors based on trend and attacker behaviour.

Risk Scoring: Label assets, users, or activities with risk levels to order responses.
Indicators of Compromise (IoC's): Leverage big data analytics to detect IoC's within network traffic and logs.

I. Contextual Threat Analysis.

Integration with External Feeds: Integrate internal data with external threat intelligence feeds to obtain wider visibility into new threats.
Contextual Analysis: Leverage natural language processing (NLP) to extract pertinent insights from unstructured sources such as emails, forums, or incident reports.
Geospatial Analysis: Identify the sources of attacks and visualize worldwide threat environments.

J. Intelligent Process Automation.

Security Orchestration, Automation, and Response (SOAR): Leverage big data insights within automated playbooks to streamline the mitigation of threats.
Incident Response: Utilize predictive analytics to inform security teams on optimal response.

K. Continuous Improvement

- Feedback Loops: Integrate incident response findings to improve analytics models and detection functionality.
- Performance Metrics: Measure the success of big data analytics in decreasing response times for attacks and enhancing threat visibility.
- Predictive Threat Detection that gets ahead of Attackers

Big data analytics employs historical trends of attacks, behavioural anomalies, and world-wide threat intelligence to detect suspicious behaviour early—frequently ahead of an attack fully materializing. Rather than merely alerting on well-known malware, it detects unusual behaviour and cross-correlates indicators of compromise (IoC's) in real time.

III. Comparative Analysis

A comparative analysis within this research context involves systematically evaluating different approaches, methodologies, and solutions for implementing big data analytics in healthcare cybersecurity threat intelligence. Here's how comparative analysis manifests in this research domain:

A. Methodological Comparisons

Analytics Approaches
Comparing rule-based security monitoring with machine learning-based threat detection, supervised versus unsupervised learning algorithms for anomaly detection, and batch versus real-time processing methodologies. The analysis would consider accuracy rates, false positive/negative ratios, and computational efficiency with various analytical frameworks.

Big Data Technologies
Systematic comparison of distributed computing platforms (Hadoop vs. Spark vs. cloud-native alternatives), various database architectures (relational vs. NoSQL vs. graph databases), and various data processing frameworks from a performance, scalability, and healthcare-specific requirements perspective.

Threat Intelligence Integration Models
Comparing various models of integrating external threat feeds, comparing centralized vs. distributed threat intelligence architectures, and comparing various correlation engines used for correlating internal healthcare data with external security indicators.

B. Performance Metrics Comparison.

Detection Capabilities
Comparing across threats for accuracy, time-to-detection, support for varied attack vectors, and capacity to detect healthcare-specific threats such as medical device compromise or exfiltration of patient data.

Operational Efficiency
Comparing resource usage, processing performance, storage needs, and overhead of maintenance for various implementation methods. This also involves comparing cloud deployments against on-premises solutions and hybrid architectures.

Compliance and Security

Assessing how various methods address healthcare regulatory compliance (DISHA, DPDP, IT Act2000), data protection practices, and industry-specific security standards.

C. Contextual Comparisons.

Variations in Healthcare Settings

System effectiveness comparison across healthcare environments: large-scale hospital chains vs. small clinics, academic medical centres vs. community hospitals, and specialty centres such as mental health or paediatric centres.

Scales of Implementation

Performance comparison between enterprise-wide vs. departmental implementations, single-site vs. multi-site setups, and differing patient population sizes

Complexity of Integration. Comparing the challenges of implementation across various existing IT infrastructures, legacy system integration needs, and vendor ecosystem compatibility.

TABLE II: LITERATURE REVIEW SURVEY

Title	Name of the Journal, Year Published	Technology used	Merits	Demerits	Performance Evaluation Accuracy	Sensitivity	Specificity
Big data analytics: a link between knowledge management capabilities and superior cyber protection	Journal of Big data. 2019	ML Algorithm	Cyber Agility	Limited real-time analysis	70%	70%	80%
An Optimized Integrated Framework of Big Data Analytics Managing Security and Privacy in Healthcare Data.	Wireless Personal Communication. 2021	ML Algorithm	Improved real-time threat detection.	Computational Complexity	75%	75%	85%
Cyber threat assessment and management for securing healthcare ecosystems using natural language processing.	IJIS 2023	NLP & ML techniques	Holistic threat management	Domain biased.	70%	70%	70%
The Enhancing Cybersecurity with AI Algorithms and Big Data Analytics: Challenges and Solutions	JTIE 2024	Apache Spark, Hadoop, AI Algorithm	High speed & detection accuracy	General rather than sector specific insights	90%	90%	90%
Big Data Analytics in Cybersecurity: Uncovering Threats, Vulnerabilities, and Attack Patterns for Prevention.	IDSA 2024	ML Algorithm	Real-time monitoring enabled through BDA	Challenges in data quality and scalability	80%	75%	75%
Leveraging Big Data Analytics in Healthcare Enhancement.	Multimedia Systems 2020	Apache Spark, Hadoop, ML Algorithm	Actionable outcome	Implementation hurdles	90%	90%	90%
Enhancing healthcare data security using RFE and CRHSM for big data." Computers in Biology and Medicine.	*Computers in Biology and Medicine* 2025	ML Algorithm	Performance at Scale	Generalizability Issue	85%	80%	90%
Cyber threat assessment and management for securing healthcare ecosystems using natural language processing	International Journal of Information Security 2023	ML Algorithm	Accurate extraction and risk assessment:	Lack of performance	80%	80%	80%
Automated detection of cyber-attacks in healthcare systems: A novel scheme with advanced feature extraction and classification.	*Computers & Security* 2025	DL Algorithm	Good performance Law errors	Dataset and environment constraints	90%	90%	90%

IV. RESEARCH GAP ANALYSIS

Gaps in research in this area point to wide opportunities for the improvement of healthcare cybersecurity defence through big data analysis. Some of the wide gaps identified are:

A. Healthcare-Specific Threat Intelligence Gaps

Medical Device Security Analytics
Existing big data analytics platforms do not adequately handle the special security risk of IoT medical devices, which communicate using various protocols and produce varying patterns of data compared to conventional IT systems. Network security activity correlation with medical device telemetry to identify device-specific attacks is not well studied.

Patient Data Flow Security
Little has been studied to date on patient data tracking and protection as it traverses complex healthcare systems with many providers, third-party utilities, and cloud infrastructures. Existing analytics strategies are not strong enough to record adequate data lineage for security in healthcare environments.

Healthcare-Specific Attack Pattern Identification
Most of the cybersecurity analytics are taken from common IT environments and do not identify patterns of attack that relate to healthcare, including modification of medical records, forgery of prescriptions, or attacks on specific medical protocols such as HL7 or DICOM.

B. Technical and Methodological Gaps

Real-Time Processing of Healthcare Data Volumes
Hospitals produce huge volumes of real-time data from patient monitoring systems, imaging equipment, and electronic medical records.
Existing big data analytics technologies are finding it difficult to keep up with the real-time processing requirements without compromising the accuracy required in health environments.

Privacy-Preserving Analytics
There isn't sufficient research being done on utilizing advanced analytics to identify threats while keeping patient information private using methods such as differential privacy, homomorphic encryption, or secure multi-party computation in the healthcare environment.

Federated Learning for Healthcare Security
Scant research on federated learning methods that would enable multiple healthcare organizations to work collaboratively developing enhanced threat detection models without sharing sensitive patient information collectively.

C. Integration and Interoperability Gaps.

Legacy System Integration
Healthcare organizations have mission-critical legacy systems, which are hard to control using new analytics features. End-to-end methodologies lack big data analytics integration and historical healthcare IT infrastructure.

Cross-Organizational Threat Intelligence Sharing
Although health organizations face the same threats, little research has been conducted on secure and privacy-preserving threat intelligence sharing across healthcare networks without jeopardizing patient anonymity.

D. Regulatory and Compliance Gaps.

Dynamic Compliance Monitoring
There is minimal existing research regarding how big data analytics can keep tracking and enforcing compliance with changing healthcare regulation and identify security events.

Automated Incident Response in Healthcare
There is minimal research on automated response systems having the ability to respond correctly in healthcare settings where system availability is vital to treating patients.

E. Evaluation and Validation Gaps

Healthcare-Specific Benchmarking
Lack of consistent standardized data sets and benchmarking criteria for evaluating the performance of cybersecurity analytics in healthcare environments, making it challenging to compare various approaches on an equal playing field.

Long-term Effectiveness Studies
Limited longitudinal studies of the long-term efficacy of big data analytics solutions to healthcare cybersecurity, including their ability to learn and adapt to emerging threats and emerging healthcare technology.

F. Emerging Technology Gaps.

Artificial Intelligence/ Machine Learning Model Explainability
Interpretable AI decision-making is needed in healthcare settings for compliance and trust but has not garnered the needed research focus on interpretable machine learning algorithms for use within healthcare cybersecurity systems.

Edge Computing Security Analytics
With increasing deployment of edge computing in healthcare (transportable devices, remote monitoring), there is minimal work on distributed analytics methods that can offer security intelligence at the edge with centralized management.
These areas of knowledge deficiency are among those areas in which targeted research can move the field significantly and offer improved cybersecurity safeguards for health care organizations and patient information

V. FUTURE SCOPE

The future course of this research has promising directions to advance healthcare cybersecurity with emerging technologies and evolving threat profiles. The key areas for future development include: Emerging Technology Integration: Artificial Intelligence and Machine Learning Development: The future study will likely explore advanced AI techniques like deep learning architectures specific to healthcare security trends, reinforcement learning for adaptive threat handling, and quantum machine learning algorithms that could process healthcare security data exponentially faster without sacrificing privacy.
Edge Computing and Distributed Analytics: With healthcare increasingly turning to edge computing for IoT medical devices and real-time patient monitoring, future research will focus on distributed threat intelligence systems that can operate across edge nodes while maintaining centralized coordination and learning capabilities.
Block chain Integration: Research will investigate block chain-based secure data sharing architectures for threat intelligence in healthcare networks, creating tamper-proof audit trails for security events and enabling trusted collaboration among healthcare organizations without compromising patient privacy.
Global Healthcare Security Standards.: Carry out research into standardized approaches to healthcare cybersecurity that are able to operate across diverse national healthcare infrastructures and regulatory regimes. The future horizon is a rich area of research potential that is set to revolutionize the manner in which healthcare organizations protect themselves and their patients against evolving cyber threats while enhancing the quality and availability of healthcare services.

VI. CONCLUSION

In short, big data analytics has the potential to provide highly effective tools for anticipatory protection of the sensitive pathology information of cancer patients. The project can be effectively utilized for both cybersecurity (DoS detection) and clinical outcomes (Cancer data analysis), can build a dual-purpose big data architecture. Cancer patients all over India are a very vulnerable group in the digital health ecosystem that are producing enormous amounts of sensitive health information through treatment tracking, diagnostic imaging, genetic tests, and telemedicine visits. This paper sketches a holistic framework for utilizing big data analytics to create proactive cyber threat intelligence networks safeguarding the cancer patient information while ensuring the accessibility and responsiveness of healthcare services. Conventional security layers are often insufficient in fighting novel-style threats. By the convergence of big data analysis, organisations can reveal hidden attack paths and react pro-actively. By adding big data analytics to your security platform, you can respond rapidly to threats, enhance situational awareness, and strike at incidents more effectively. Big data analytics is a breakthrough method for performing healthcare cybersecurity threat intelligence. By leveraging powerful analytics techniques, healthcare organizations can transition from a reactive to a proactive security posture, more securely protecting sensitive patient data while maintaining operational efficiency and leverage cancer patient records for clinical insights, early diagnosis, and personalized treatment prediction.
Finally, safeguarding cancer patients' pathology information takes both technology and governance: strong analytics to detect anomalies, and solid policies (encryption, access controls, audit trails) to meet national and international standards. Success lies in implementing an enterprise strategy that brings together technology,

process, and people with stringent compliance to healthcare laws and patient privacy requirements. Organizations must start by testing programs in high-impact application areas and build up analytics capabilities in steps as they acquire skills and demonstrate value. Through the rollout of these big data analytics programs, healthcare organizations can prevent, detect, and respond to cyber threats, thus safeguarding sensitive patient information and meeting regulatory requirements

REFERENCES

[1] Obitade P O, "Big data analytics: a link between knowledge management capabilities and superior cyber protection," Journal of Big Data, vol.6, pp.1-15, Aug. 2019. DOI: https://doi.org/10.1186/s40537-019-0229-9

[2] Chauhan R, Kaur H & Chang V, "An Optimized Integrated Framework of Big Data Analytics Managing Security and Privacy in Healthcare Data," Wireless Personal Communications ,vol.117, no.1, pp.87–108, Oct.2021 DOI: https://doi.org/10.1007/s11277-020-07040-8

[3] Islam S, Papastergiou S, & Silvestri S, "Cyber threat assessment and management for securing healthcare ecosystems using natural language processing," International Journal of Information Security, vol.23,no.1,pp. 31–50,Jul.2023. DOI: https://doi.org/10.1007/s10207-023-00769-w

[4] Nugroho S.A, Hadi A.P, & Sumaryanto, "The Enhancing Cybersecurity with AI Algorithms and Big Data Analytics: Challenges and Solutions," Journal of Technology Informatics and Engineering (JTIE), vol.3, no.3, pp. 279–295,Dec.2024 DOI: https://doi.org/10.51903/jtie.v3i3.200

[5] Hossain N, & Kamal N, "Big Data Analytics in Cybersecurity: Uncovering Threats, Vulnerabilities, and Attack Patterns for Prevention," Intelligent Data Science and Analytics, vol.1, no.1, pp. 23–3, Jan 2024. DOI:https://doi.org/10.63110/idsa.v1i01.4 .

[6] Saraf K.R, & Malathi P, " Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare," International Journal of Intelligent Systems and Applications in Engineering,vol.11,no.2,pp. 537–549 , 2023 DOI:https://ijisae.org/index.php/IJISAE/article/view/2709

[7] Arshia Rehman, Saeeda Naz, & Imran Razzak, "Leveraging Big Data Analytics in Healthcare Enhancement: Trends, Challenges and Opportunities," Multimedia Systems , vol.28, no.4, pp. 1339–1371, Jan 2021 DOI:https://doi.org/10.1007/s00530-020-00736-8

[8] Mamta, Brij B.Gupta, Kuan Ching Li, Victor C. M. Leung, Kostas E. Psannis, Shingo Yamaguchi, "Block chain Assisted Secure Fine Grained Searchable Encryption for a Cloud Based Healthcare Cyber Physical System," IEEE/CAA Journal of Automatica Sinica,vol.8,no.12,pp. 1877–1890,Dec.2021. DOI: https://doi.org/10.1109/JAS.2021.1004003 .

[9] C. Sreedhar, K. Mahesh Babu, S. Kallam, G.S. Pradeep Ghantasala, S. Anthoniraj, S. Kumarganesh, K. Martin Sagayam, B.K. Pandey, D. Pandey, "Enhancing healthcare data security using RFE and CRHSM for big data," Computers in Biology and Medicine.Elsevier, vol.189, may 2025. DOI:https://doi.org/10.1016/j.compbiomed.2025.110063

[10] Seshagirirao Lekkala, Raghavaiah Avula & Priyanka Gurijala,"Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity," Journal of Artificial Intelligence and Big Data,vol.2,no.1,pp. 32–48 ,Mar.2022, Volume 2, Issue 1,32-48. DOI: https://doi.org/10.31586/jaibd.2022.1125