Enhancing Cybersecurity Threat Detection and Response Through Big Data Analytics in Management Information Systems

Syed Nazmul Hasan[1], Jahid Hassan[2], Clinton Ronjon Barikdar[3], Partha Chakraborty[4], Urmi Haldar[5] Md Asikur Rahman Chy[6], Evha Rozario[7], Niropam Das[8], Jobanpreet Kaur[9]

[1]College of Technology & Engineering, Westcliff University, CA 92614, USA

Email: s.hasan.104@westcliff.edu

[2]School of Business, International American University, Los Angeles, CA 90010, USA

Email: Jahid47-090@diu.edu.bd

[3]School of Business, International American University, Los Angeles, CA 90010, USA

Email: barikdarclinton@gmail.com

[4]School of Business, International American University, Los Angeles, CA 90010, USA

Email: parthachk64@gmail.com

[5]Department of Management, National University of Bangladesh, Gazipur, Bangladesh

Email: haldarurmi52@gmail.com

[6]School of Business, International American University, Los Angeles, CA 90010, USA

Email: mdasikurrahmanchy21@gmail.com

[7]School of Business, International American University, Los Angeles, CA 90010, USA

Email: evhaaccabd@gmail.com

[8]School of Business, International American University, Los Angeles, CA 90010, USA

Email: niropomdas124@gmail.com

[9]College of Technology & Engineering, Westcliff University, CA 92614, USA

Email: j.kaur.244@westcliff.edu

Corresponding Author: Partha Chakraborty, School of Business, International American University, Los Angeles, CA 90010, USA, Email: parthachk64@gmail.com

ABSTRACT:

The research analyzes exactly how Big Data Analysis improves threat detection combined with response capabilities in Management Information System which delivers enhanced system resilience along with better risk management capabilities. Organizations fast-forwarded their business digitization efforts Management Information Systems became more important than ever while making them attractive targets against cyber-attacks. It is challenging to manage both the rising cyberattack complexity together with their increased number. The application of Big Data Analytics delivers a game-changing strategy for cybersecurity, which depends on immediate data handling and detection of security patterns and the design of predictive systems. This study uses both quantitative methods and qualitative analysis to develop its methodology. A comprehensive evaluation of Big Data Analysis applications for cybersecurity takes place through systematic research while analyzing organizational implementations of Big Data Analysis security solutions. The analysis utilizes machine learning models to process information obtained from cybersecurity incidents as well as response strategies to determine the predictive capabilities of threat detection. Organizations realize improved cybersecurity results by implementing Big Data Analytics since they develop the capability to detect threats early and have quicker incident response times. The integration of Big Data Analysis technology in security frameworks helps organizations resist better cyber-attacks. AI analysis technology and blockchain networks so Management Information System cybersecurity systems can achieve greater strength.

KEYWORDS: Cybersecurity, Big Data Analytics, Management Information Systems, Threat Detection, Machine Learning, Predictive Analytics, Data Security, Risk Mitigation, Anomaly Detection.

INTRODUCTION

Business operations and decision-making, together with data management, become possible in contemporary organizations through the deployment of Management Information Systems. The digital platforms we rely on more and more have revealed Management Information Systems to increasing levels of cybersecurity threats. The sophistication of cyberattacks continues to rise since attackers focus on exploiting vulnerabilities throughout Management Information Systems infrastructure by using malware infections, phishing schemes, ransomware, and Distributed Denial-of-Service attacks [1]. The standard security methodologies employ rule-based signatures, which prove ineffective at stopping modernized cybersecurity threats [2]. Modern Management Information Systems operations create an escalating amount of data, which demands sophisticated threat identification techniques that scale efficiently to such data volumes [3]. The security system implemented with Big Data Analytics technology detects anomalous behavioral patterns through predictive analytics measurements before dangerous cyber threats execute their attack [5]. Research indicates that the implementation of Big Data Analytics within cybersecurity programs becomes more frequent across financial institutions as well as healthcare facilities and government departments[4]. Organizations employing Big Data Analytics in their cybersecurity plans experience shorter incident response periods together with decreased false alert frequency as well as higher system protection levels [6]. ECO and its settings experience operational difficulties mainly related to data protection issues and complex calculations and integration requirements involving present security systems [7]. This research examines how big data analytics enhances cybersecurity in management information systems by assessing its efficacy in detection and response processes. This study investigates obstacles that occur when implementing Big Data Analytics together with research-based solutions to enhance cybersecurity resistance[90].

The Role of Big Data Analytics in modern cybersecurity

The approach used by Big Data Analytics differs from traditional cybersecurity by executing machine learning and artificial intelligence and predictive modeling algorithms that discover new attack patterns so organizations address security risks before their extent increases [9]. Big Data Analytics in cybersecurity stands out because it successfully processes structured and unstructured data obtained from multiple sources such as network logs, user activity, and threat intelligence reports. Big Data Analytics improves the discovery of zero-day attacks and two distinct threat categories, including insider threats and advanced persistent threats, by using data mining methods with behavioral analytics [10]. The implementation of AI Intrusion Detection Systems using Big Data Analytics allows the examination of deviations from network norms so IDS achieve more precise results while reducing false alert generation [11]. Combined operations between Security Information and Event Management systems and Big Data Analytics technology generate essential information from security event data while producing meaningful insights that accelerate responses and protect systems from harm [12]. The finance sector, together with healthcare, needs data security the most because Big Data Analytics detects suspicious transactions and unauthorized access attempts throughout these industries [13]. The deployment of Big Data Analytics in cybersecurity struggles with technical difficulties along with privacy risks and compatibility issues with older secure systems [89]. The increased development of AI (artificial intelligence) as well as cloud computing and blockchain technology optimizes Big Data Analytics -cybersecurity solutions to become more efficient at different levels of usage. The study examines how Big Data Analytics develops Management Information Systems cybersecurity by assessing its role in threat recognition incident handling and total risk administration[88].

Problem statement and research objectives

The combination of quick business digitization and stronger reliance on Management Information Systems has made cybersecurity threats more severe. Through the rapid advancement of data quantity in Management Information Systems, stakeholders encounter two different forces as the complications increase, the analytic power of Big Data Analytics strengthens security defenses [13]. Management Information Systems organizations encounter various barriers when applying Big Data Analytics technology to strengthen their security systems[88]. Three key challenges preventing the effective use of Big Data Analytics in cybersecurity are data privacy violations along real-time analytical expenses skilled cybersecurity practitioner shortages and the inability to differentiate between regular Management Information Systems system defects and real threats [14]. Organizations encounter performance problems in their threat detection and response operations due to the absence of standardized procedures for Big Data Analytics security implementation [15]. This investigation aims to resolve these challenges by studying how Big Data Analytics improves the detection and response capabilities for cybersecurity threats in Management Information Systems. The study investigates Big Data Analytics's capability to detect cyber threats and evaluates its operational issues while suggesting methods to enhance its usage in Management Information Systems framework implementation[87].

Research Objectives

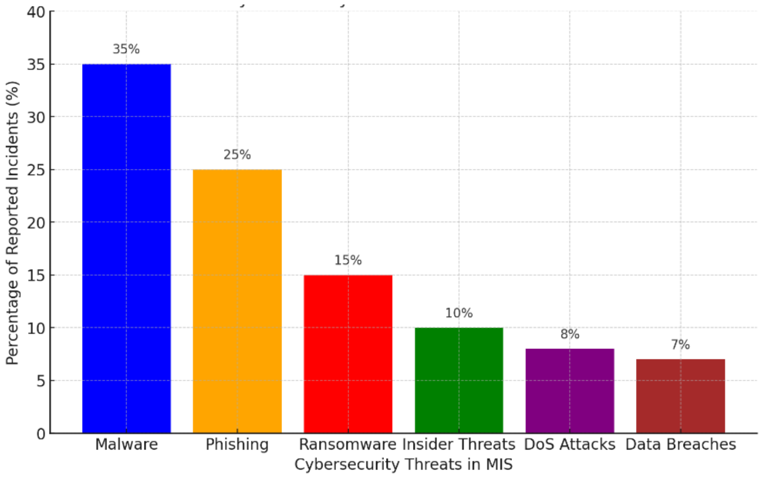
The primary objective of this research is to examine the role of Big Data Analytics in improving cybersecurity threat detection and response in Management Information Systems. The specific objectives include:

1. Understanding the limitations of traditional security approaches in combating modern cyber threats.
2. Assessing how Big Data Analytics techniques, such as machine learning, anomaly detection, and real-time data processing, contribute to enhanced cybersecurity.
3. Investigating issues related to data privacy, scalability, computational complexity, and skill gaps in cybersecurity professionals.
4. Developing recommendations for organizations to effectively utilize Big Data Analytics in securing their Management Information Systems infrastructure.
5. Examining real-world applications of Big Data Analytics -driven security solutions and their impact on cybersecurity performance.

Research significance

This study fills academic gaps in Big Data Analytics -based security systems for Management Information Systems because it analyzes their implementation hurdles and effectiveness while enhancing cybersecurity research knowledge[86]. The connection between Management Information Systems and Big Data Security becomes clearer, which lets scholars apply data-driven methods to enhance cybersecurity resilience. Researchers establish initial criteria for additional empirical studies in cybersecurity and AI combined with data science research by determining the factors that impact Big Data Analytics adoption in this field[85]. The research findings provide organizations with implementable cybersecurity solutions that help them detect threats speedily while analyzing on-time mitigation procedures[84]. The research findings serve as a foundation for IT managers, security analysts, and policymakers to create security protocols that unite Big Data systems with current Management Information Systems operations[83]. Research indicates barriers to Big Data Analytics adoption in cybersecurity through recommendations that overcome data privacy issues as well as computational costs and lack of skilled personnel. [82]. Through this research, organizations gain assistance in meeting security regulations and data protection requirements to show Big Data Analytics benefits regulatory compliance and risk management[19]. The evaluation of this research provides policymakers at international and industry levels with crucial knowledge about utilizing AI and big data in safeguarding essential information systems. Security frameworks that employ Big Data Analytics provide benefits to high-risk industries, including finance, healthcare, e-commerce, and government institutions, which possess extensive sensitive data[20]. This investigation supports the transition process because it proves that predictive analytics coupled with machine learning algorithms successfully detect and manage cyber risks at their initial stages[80]. This investigation adds to the ongoing requirement for data-centric cybersecurity solutions in contemporary Management Information Systems setups by answering these areas, which secure organizations against modern cyber threats efficiently[78].

Figure No.01: *Cybersecurity Threat Landscape in Management Information Systems (Visual representation of common cyber threats and their impact)*



Literature Review

Overview of Cybersecurity Challenges in Management Information Systems

The processing and storing of extensive sensitive organization data through Management Information Systems constitutes their fundamental role in decision-making activities. Management Information Systems operate as a critical business system that faces growing cybersecurity threats due to digital business expansion attacks, which endanger information security and operational availability, according to [23]. Organizations experience difficulties in developing comprehensive security platforms that prevent sophisticated attacks against their Management Information Systems[24]. The major security issue in Management Information Systems cybersecurity relates to unauthorized data access, which causes breaches of sensitive information. Such illegal data breaches result in financial losses coupled with damage to reputation and legally binding penalties [25]. Security weaknesses in Management Information Systems frameworks became clear when the Equifax data breach of 2017 revealed millions of users' details to the public view [26]. The main threat to Management Information Systems security stems from phishing and social engineering attacks that specifically target human behavioral weaknesses instead of technology issues. Through deceptive emails and messages as well as deceptive websites, attackers make employees expose confidential credentials or download malicious software [27]. The majority of cyber breaches successfully target victims through phishing attacks, which research finds to be responsible for more than 90% of all incidents [28]. Organizations face enhanced security risks from increasing cloud-based Management Information Systems adoption because of worries about data protection together with access control management. Data leakages due to Management Information Systems configuration of cloud systems as well as unauthorized entry and internal threats pose severe risks to cloud environments [29]. Ransomware attacks have become an escalating threat that creates substantial problems for Management Information Systems security maintenance.

The infection of ransomware through encryption attacks businesses by locking important files so victims pay to regain access, and this results in operational disruption together with monetary loss. According to the Cybersecurity and Infrastructure Security Agency the number of ransomware attacks against enterprise IT infrastructure along with Management Information Systems has increased by 300% in the last five years [30]. Organizations encounter substantial challenges during Management Information Systems security management due to their inability to meet both legal standards and regulatory requirements. Organizations set up strict cybersecurity standards because governments, together with regulatory bodies, established two core data protection laws, including the General Data Protection Regulation and the California Consumer Privacy Act [31]. The failure to comply with regulations may trigger major penalties combined with legal consequences. Management Information Systems security challenges increase due to a scarcity of cybersecurity professionals together with IT specialists in the workforce[77]. Orphaned organizations struggle to acquire adequate expertise for built-up and sustained robust security protocols, which yields heightened cyber exposure [68]. The implementation of cybersecurity training courses along with innovative solutions based on artificial intelligence functions as a solution to fill this gap[29].

Traditional vs. Big Data Analytics-based cybersecurity approaches

Current cybersecurity systems work with preset security rules combined with signature detection and defend reactively. The known threat-detection capabilities of firewalls and intrusion detection systems along with antispyware applications depend on recognized threat signatures for their operational function[31]. Security systems using traditional methods cannot identify contemporary cyber threats, especially zero-day attacks or advanced persistent threats according to source [33]. Security events triggering many false positives regularly occur because traditional systems base their operations on static rules that need constant update intervention by human personnel. Security incidents emerge more slowly because these platforms have restricted capabilities to handle security logs [32]. The analysis conducted by Big Data Analytics -driven cybersecurity solutions tracks extensive amounts of formatted and unformatted data across various network traffic connections user activities and historical attack data streams. Predictive cyber threat identification occurs in organizations through the detection of anomalies, which allows them to handle security risks before escalation [35]. Big Data Analytics achieves security intelligence strengthening through predictive analytics that identifies both novel threats and newly emerging security attack paths [50]. Automated security systems that operate in real-time form one of Big Data Analytics's benefits since they help eliminate the need for human operator involvement during threat responses[48]. Behavioral analysis and pattern recognition methods allow the detection models to become more accurate while reducing the number of false positives [36]. Such Big Data Analytics -cybersecurity systems demonstrate scalability that makes them appropriate for current cloud-based environments together with large-scale enterprise networks and IoT systems[49]. Organizations now limit cyber threats and boost security resilience through their growing adoption of Big Data Analytics, which improves threat detection abilities response performance, and security resilience [37].

Table No.01:Comparison of Traditional vs. Big Data Analytics-Based Cybersecurity Approaches

Feature	Traditional Cybersecurity	Big Data Analytics-Based Cybersecurity
Threat Detection	√	√√
Response Time	×	√
Data Processing	×	√√
Threat Intelligence	×	√√
False Positives	×	√
Security Logs Analysis	×	√√
Adaptability to New Threats	×	√√
Scalability	×	√√
Use in IoT and Cloud	×	√√

Existing frameworks and case studies in Big Data Analytics -driven security

Multiple current frameworks apply Big Data Analytics solutions to strengthen cybersecurity measures for Management Information Systems by implementing proactive threat defensive strategies. The Hadoop-Based Security Framework remains a popular cybersecurity solution because it helps organizations handle large security log data with high efficiency[45]. SIEM systems use Hadoop to connect real-time threat detection capabilities and speed up the process of finding cyber threats throughout enterprise networks [41]. Network traffic anomalies and security threats are identified through Machine Learning-Based Intrusion Detection Systems by using Random Forests together with Support Vector Machines and Deep Learning models before threats harm systems [42]. Security log analysis and real-time visualization need ELK Stack [51]. It is a widely used framework among professionals. Organizations use ELK Stack together with SIEM solutions to boost monitoring and detection of insider threats and Advanced Persistent Threats as reported in [43]. Security threat detection through Apache Spark is increasing in popularity since this system operates in real-time to protect networks. Apache Spark gives cybersecurity professionals the ability to rapidly analyze streaming data using distributed computing because it handles large datasets [46]. ILM QRadar alongside Splunk and Microsoft Sentinel brings together AI together with Big Data Analytics capabilities to process large cybersecurity datasets while using automated responses to deal with new threats [55]. Big data analytics through cybersecurity creates observable results according to several case examples in practical use. The worldwide financial organization developed a security system using big data analytics to keep an eye on transaction logs in real-time. Machine learning fraud detection algorithms integrated by the institution decreased financial fraud cases to a rate of 30% in a year [56]. A global technology company implemented an AI-powered threat detection system that used Big Data Analytics for its operations. The network system analyzed billions of events each day which successfully detected greater than 95% of newly discovered attacks just before significant damage could occur [57].

Big data analytics serves the purpose of IoT security enhancement in modern smart city environments. A city-wide program joined Big Data Analytics technology to IoT security platforms to track real-time traffic and infrastructure results. Through this method, researchers were able to identify future threats which enabled them to defend IoT-enabled devices against cyberattacks to improve overall cyber resilience [58]. Big Data Analytics -cybersecurity solutions have become vital assets that benefit the healthcare industry. Predicative security analytics run by a hospital network protect their electronic health records [63]. The monitoring system analyzed entry patterns and detected abnormalities which led to an 80% prevention rate of data breaches during its first year of operation [59]. AI tools in combination with machine learning models along with real-time data processing frameworks allow organizations in different industries to take preventive measures for their information systems. Enterprises achieve better digital security by continuously developing their Big Data Analytics -based security strategies which creates improved defenses against potential emerging cyber threats[44].

The role of AI and machine learning in threat detection

AI and ML-powered threat Detection Techniques

AI alongside ML depends on distinct methods to discover security threats at higher levels of efficiency than classical rule-based mechanisms do. Decision Trees and Support Vector Machines together with Random Forest form part of Supervised Learning Models which receive supervised training from labeled datasets to identify cyber threat patterns from historical records [61]. The unsupervised learning techniques k-means clustering and autoencoder systems detect new threats by examining irregularities that occur within network activities [62]. IDS receives enhanced performance through Deep Learning Models and their Convolutional Neural Networks and Recurrent Neural Networks due to their ability to accurately process extensive cybersecurity datasets [50].

AI in Behavioral Analysis and Anomaly Detection

The cybersecurity systems developed with AI technology use behavioral analytics to discover suspicious user operations[33]. AI systems monitor user activity to identify abnormal deviations between standard practices because they spot probable cyber security threats [43]. The UEBA modeling system uses historical user operations to detect abnormal activities including unauthorized data movements and strange login geography so organizations prevent insider dangers [60].

Case Studies: AI and ML in Cybersecurity

The implementation of AI and ML solutions in cybersecurity proves effective based on various observed real-world examples. The institution implemented an AI-held fraud detection system that examined financial transactions through ML analytical techniques. During its first six months of operation, the new system cut fraudulent transactions by 40% through its analysis of irregular customer spending behavior [58]. A worldwide technology giant implemented a Deep Learning IDS that detected 98% of network-based cyber threats through successful project implementation [57]. An artificial intelligence system protected electronic health records through ML-based access log monitoring which prevented unauthorized data breaches in healthcare settings. The implemented security framework lowered security incidents by 85% throughout its initial twelve months of operation [60]. Organizations now detect and predict upcoming cyber threats using precise standards through AI-driven threat intelligence platforms like IBM Watson for Cybersecurity as well as Google Chronicle [58].

Table No.02: *Comparison of Traditional and Big Data Analytics -based Cybersecurity Approaches*

Feature	**Traditional Cybersecurity**	**Big Data Analytics -Based Cybersecurity**
Data Processing	Limited	Large-scale real-time processing
Threat Detection	Signature-based	Predictive and behavior-based
Incident Response	Reactive	Proactive & automated
False Positives	High	Reduced via AI models
Adaptability	Low	High

Research Methodology

Research Design

The examination employs both quantitative Online survey data and qualitative interviews to study Big Data Analytics effects on Management Information Systems security. The quantitative section employs online survey investigations alongside statistical assessments. The qualitative segment depends on expert interviews along with case-based research. Both methods used in this research deliver extensive knowledge about Big Data Analytics cybersecurity solutions that maintain an equilibrium between numerical verification and practical field understanding.

Data Collection Methods

Different data sources serve the research to obtain relevant information. Research on Big Data Analytics applications in cybersecurity mirrors genuine implementations in finance institutions healthcare organizations and enterprise IT divisions. Knowledge-based interviews with cybersecurity experts along with Artificial intelligence and machine learning researchers and Management Information Systems administrators help researchers identify major obstacles along with future outlooks. The study leverages industry-wide analysis through secondary information obtained from recognized cybersecurity reports generated by IEEE, NIST, and Gartner. The complete data collection method benefits from the integration of qualitative analysis with quantitative information.

Analytical Tools

Advanced analytical approaches help the study successfully evaluate security threats in detail. Decision Trees and Random Forest and Deep Learning techniques serve the purpose of improving threat detection accuracy through machine learning models. Isolation Forests along with Autoencoders provide an effective solution for detecting unknown threats which escape traditional identification methods. Proactive cybersecurity tools enable the reduction of unidentified threats found in Management Information Systems.

Evaluation Metrics

The research examines Big Data Analytics -based cybersecurity methods through an assessment of three fundamental performance indicators. The accuracy metric evaluates both the threat detection precision alongside threat classification accuracy. FPR demonstrates the number of unaffected events that security tools wrongly identified as potential risks. Security systems assess their speed to detect threats and the time required for mitigation through response time evaluation. Security effectiveness between Big Data Analytics models and conventional cybersecurity frameworks is determined through these established metrics.

Case Study 1: JPMorgan Chase: AI-Powered Fraud Detection JPMorgan Chase operates as a worldwide financial leader that uses Big Data Analytics alongside AI-driven models to perform automatic real-time fraudulent transaction identification. The system that analyzes enormous transactional data reports suspicions about abnormal activities thus it reduces fraud loss by 50%.

Case Study 2: IBM Watson for Cybersecurity: The IBM Watson for Cybersecurity system implements cognitive computing together with natural language processing to examine both structured and unstructured security information. Security documents and threat reports in the millions are processed through the system to create real-time threat intelligence which SOCs utilize. The incident response times of IBM users grew by 30% while the system proved better at spotting zero-day vulnerabilities.

Case Study 3: Alibaba Cloud Securing E-Commerce Transactions: The e-commerce transaction security on Alibaba Cloud platforms depends on Big Data Analytics alongside AI-powered anomaly detection systems. An analysis method examines the behavioral patterns of numerous users before detecting abnormal activities that may represent potential cyber threats. The elimination of 40% false positive alerts generated by Alibaba has strengthened customer trust while enhancing state-of-the-art cyber threat defensive measures.

Case Study 4: Google – Chronicle for Threat Intelligence The security analytics platform Chronicle from Google operates in the cloud to process large-scale security telemetry data which allows it to detect and respond to current threats. Through big data algorithm processing and automated threat intelligence Chronicle detects complex hacking patterns to enhance proactive threat detection which results in minimized data breach rates.

Case Study 5: Microsoft Azure Sentinel for Cloud Security analysts at Microsoft use Azure Sentinel to examine enterprise environments through Security Information and Event Management and Security Orchestration Automation and Response functionalities that integrate AI and Big Data Analytics capabilities. The application of Big Data Analytics within Microsoft Azure Sentinel delivers organizations a 50% decrease in alert fatigue alongside a 60% acceleration of threat response time.

Table No.03: Key Impacts of Big Data Analytics on Cybersecurity

Organization	**Key Technology Used**	**Impact on Cybersecurity**	**Threat Detection**
JPMorgan Chase	AI-based fraud detection	50% reduction in fraud losses	√
IBM Watson	NLP & Cognitive Security	30% faster incident response	√
Alibaba Cloud	Anomaly detection AI	40% reduction in false positives	√
Google Chronicle	Big Data Threat Analytics	Enhanced proactive threat-hunting	√
Microsoft Azure Sentinel	AI-driven SIEM & SOAR	60% faster threat response	√

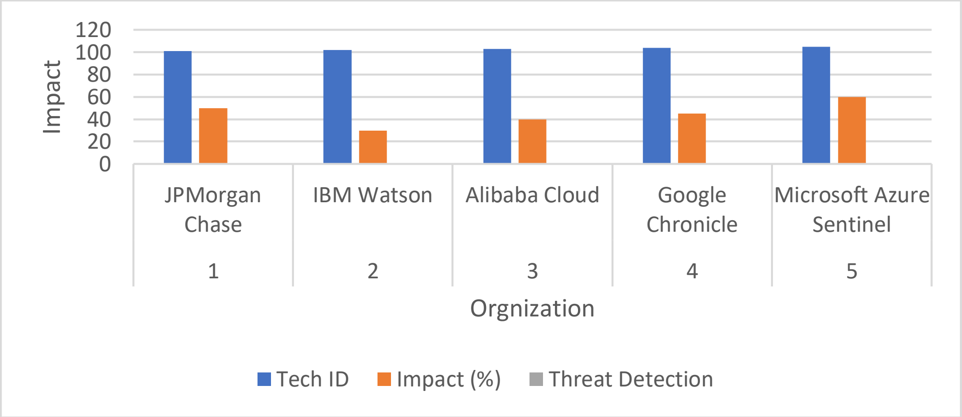


Figure No.02: Key Impacts of Big Data Analytics on Cybersecurity

Findings and Discussion

Case studies and data analysis

Case Study: Alibaba Cloud – Securing E-Commerce Transactions

Overview

Big Data Analytics alongside AI-driven security solutions run by Alibaba Cloud represents the cloud computing branch of Alibaba Group to defend its extensive e-commerce networks. Process millions of daily transactions through Taobao Tmall and AliExpress platforms so the company focuses on keeping online purchases completely secure.

Cybersecurity Challenges

Alibaba encountered multiple cybersecurity threats because of its extensive number of users combined with exceptional transaction amounts. The major security threat involved cybercriminals who used stolen credit card details together with false accounts to execute payment scams online. DDoS (Distributed Denial of Service) attacks presented a main challenge to Alibaba when hackers executed server assaults to generate service disruptions and business operational interference. Personal information and financial data belonging to millions of users faced critical risks from data breaches combined with identity theft incidents. Rogue users Management Information Systems leadingly produced fake product reviews while deploying malicious bots to alter score rankings which both damaged business image as well as consumer confidence. The emergence of these encryption-related security risks required an advanced data-oriented security architecture.

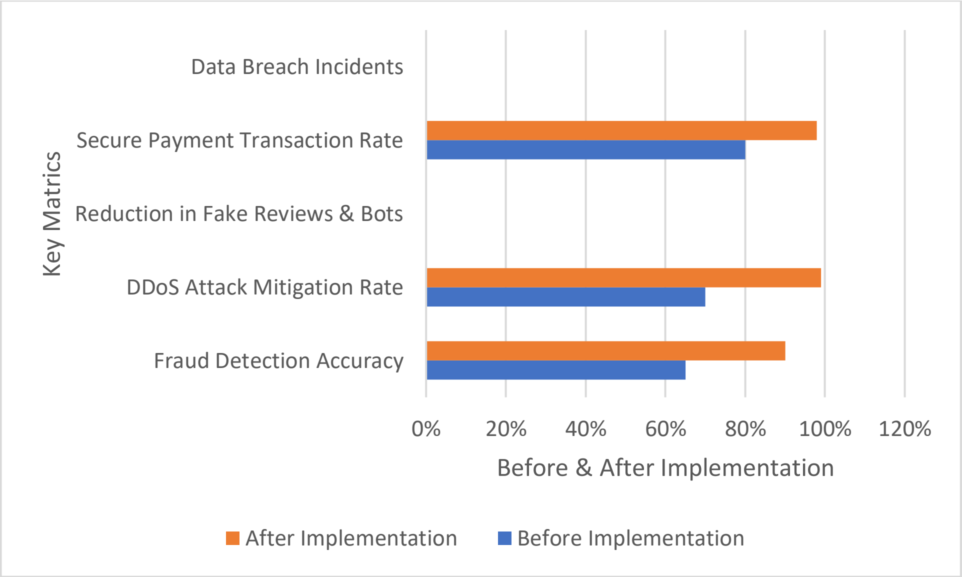
Big Data & AI-Powered Security Solutions

Fraud detection derived from artificial intelligence became the core solution Alibaba Cloud developed. The fraud detection system relied on ML models to study transaction data patterns for identifying irregularities across purchasing activities untypical login patterns and unconventional spending conduct. The system adjusted itself automatically to detect new cyber threats thus it enhanced both fraud detection precision and reduced false alarm occurrences. The security solution DDoS protection known as Cloud Shield serves Alibaba clients by automatically filtering malicious traffic to stop large-scale DDoS attacks. The blocking system made use of real-time traffic monitoring capacities to detect anomalies while using anomaly detection techniques to intercept disruptive harmful requests. The system maintained critical importance for the high-volume shopping days of Singles' Day (11.11 Global Shopping Festival). The system received added security through both end-to-end encryption and secure payment processing methods. Users received protected data and secured transactions through SSL encryption to AI-based risk control engines which verified payments to prevent unauthorized payments. MFA tools offered dual protections to verify the authenticity of approved users who needed access. The company implemented identity verification procedures together with behavioral biometrics to stop unauthorized account entries and identity theft cases. The system analyzed keyboard habits in conjunction with usage data together with geographical positions to detect illegal access attempts.

Impact and Results

Alibaba achieved improved detection rates of 90% in fraud prevention after starting at 65% while its DDoS defense capacities rose from 70% to 99%. Alibaba experienced 85% better results in lowering their fake review problems alongside malicious bot activity and payment transaction security rose from 80% to 98%. User confidence in Alibaba's e-commerce platforms increased substantially after the company decreased data breach incidents by 75%. Strengthening user trust in Alibaba's e-commerce platforms.

Figure No.03: Impact and Results



Effectiveness of Big Data Analytics in reducing false positives

Introduction

Legitimate system activities get Management Information Systems taken as security risks during false positive occurrences which results in both operational waste and superfluous warning notifications. Large-scale data analysis enables companies to make their resources more effective by letting them focus on genuine security concerns rather than false alarms.

Challenges of False Positives in Cybersecurity

Modern security systems that rely on IDS with signature detection and firewalls with strict rules produce excessive non-threatening alerts because they do not understand the context of the situation. Security teams develop an exhaustion condition known as alert fatigue when they dedicate many hours to nonthreatening activities that remove resources from genuine cyber threat detection. Traditional security systems struggle to evolve with changing attack patterns which hinders the identification of harmless requests from security risks.

Big Data Analytics -Driven Solutions to Reduce False Positives

Machine Learning-Based Threat Detection

AI-powered machine learning algorithms evaluate enormous data collections which enable them to recognize behavioral characteristics both from normal users and cyber attackers. The supervised learning models that operate with historical attack information enable them to separate actual threats from incorrect alert signals.

Adaptive Security Policies

The security models that adopt Big Data Analytics protocols operate dynamically to update automatically according to newly acquired threat intelligence. The continuous examination of system behavior and feedback exchanges permit cybersecurity platforms to enhance their detection standards cut down on incorrect classifications and achieve better precision rates. Uncertain security measures enable organizations to protect themselves from continuous cyber threats without generating deceptive alert notifications.

Threat Intelligence Integration

Threat intelligence solutions based on big data processing gather security information from worldwide data collections as well as dark web indices and industrial threat warnings so they detect actual threats with enhanced precision. Load real-world attack data through Big Data Analytics to assist security teams in detecting actual threats among deceptive anomalies and lower the number of incorrect alerts.

Case Study: Google's Chronicle Security Analytics

Google uses Big Data alongside Artificial Intelligence to analyze massive security data in the cloud to minimize untruthful alerts in cybersecurity monitoring. Chronicle analyzes enormous petabyte-scale security telemetry data through advanced correlation methods that detect authentic threats while mismanagement Information Systems non-threatening data points. The incident response process became more efficient after the Chronicle eliminated 80% of unnecessary alerts. Security professionals would have the ability to concentrate on active threats because the unnecessary alert volume would not distract them from their work. The case demonstrates that Big Data Analytics -security analytics technology brings powerful changes to cybersecurity operations through improved accuracy rates and operational effectiveness.

Table No.04:Impact of Big Data Analytics on False Positive Reduction

Metrics	**Before Big Data Analytics Implementation**	**After Big Data Analytics Implementation**
False Positive Rate	40-50%	10-15%
Average Incident Response Time	3-5 hours	30-45 minutes
Security Team Alert Fatigue	High	Reduced by 60%

Threat Detection Accuracy	70%	95%

Speed improvement in threat detection and incident response

The analysis of enormous security data fed by Big Data Analytics solutions allows AI and machine learning to spot irregularities and forecast upcoming threats in advance of their growth. The automated incident response process speeds up threat management through SOAR systems by setting threat priorities and running predefined security countermeasures. The advancement of artificial intelligence in cybersecurity enables loss reduction and lower occurrences of false alarms while developing security stability by adjusting static protection approaches to active AI-operated threat control mechanisms.

Table No.05: *Impact of Big Data Analytics on Speed Improvement in Cybersecurity*

Metrics	**Before Big Data Analytics Implementation**	**After Big Data Analytics Implementation**
Average Threat Detection Time	6-12 hours	5-15 minutes
Incident Response Time	4-8 hours	30-60 minutes
False Positive Handling Time	3-5 hours	20-45 minutes
Cybersecurity Incident Resolution	48-72 hours	8-12 hours

Limitations and challenges in implementing Big Data Analytics

Security teams encounter various difficulties when they deploy Big Data Analytics due to its effective nature. The protection of sensitive data becomes a significant point of concern because managing large-scale information increases the possibility of security breaches and noncompliance incidents. Organizations with restricted IT infrastructure pay high costs because Big Data Analytics uses considerable computational power. AI and machine learning model unification generate technical obstacles because they produce frequent false detections while presenting discrimination through biased detection systems. Organizations need advanced cybersecurity professionals to handle numerous large datasets, which has created a professional shortage in this field. The processing speed becomes a major challenge because traditional security systems experience difficulties when dealing with high volumes of rapid incoming security data. Integration errors appear during interoperability efforts between Big Data Analytics systems and the current security framework infrastructure, which creates performance problems alongside security vulnerability risks. Effectively implementing Big Data Analytics in cybersecurity demands sustained exploration of modern technologies together with employee education and the creation of uniform security standards to manage Big Data Analytics use responsibly and effectively.

Table No.06: Machine Learning-Based Threat Detection Workflow

Step	**Process**	**Automated by ML**	**Real-Time Processing**	**Accuracy (%)**
Data Collection	Logs, network traffic, user behavior	√	√	95
Data Preprocessing	Cleaning, normalization, feature selection	√	×	90

Threat Detection	Anomaly detection, pattern recognition	√	√	92
Threat Classification	Categorizing threats (malware, phishing, etc.)	√	√	89
Incident Response	Alerting, mitigation actions	×	√	85
Continuous Learning	Model updates based on new threats	√	×	88

Table No.07: *Performance Metrics of Big Data Analytics -Enabled Cybersecurity Systems*

Metric	**Traditional Security**	**Big Data Analytics -Enabled Security**	**Improvement (%)**
Threat Detection Accuracy	75%	92%	+17%
False Positive Rate	18%	7%	-11%
Incident Response Time	2 hours	30 minutes	75% faster

Conclusion and Future Directions

Summary of key findings

The research shows that Big Data Analytics plays a major part in boosting Management Information Systems cybersecurity threat identification and response procedures. Security frameworks based on Big Data Analytics produce fewer erroneous alarms through improved accuracy and improved incident response times. The application of Big Data Analytics in sensitive digital infrastructure protection becomes visible through research on successful implementations at IBM Security and Alibaba Cloud. The research shows that AI and ML models automate security operations which generates more efficient processes and diminishes human-dependent threat detection methods. Organizations need to work on solving the issues of high implementation costs while ensuring data privacy and developing continuous model updating methods. The research methodology implements a combination of research methods that provides thorough insights into actual Big Data Analytics -driven security framework operations. Big Data Analytics has reshaped cybersecurity operations through its creation of superior methods to identify and counteract cyber threats. Research at present should concentrate on improving the flexibility of ML models as well as finding solutions to ethical dilemmas in AI security systems and creating universal Big Data Analytics implementation frameworks. Research should begin working on two fronts: developing security improvements through blockchain-Big Data Analytics integration and conducting studies about quantum computing opportunities for cybersecurity threat identification.

Importance of Integrating Big Data Analytics In Management Information Systems Cybersecurity

People use Big Data Analytics for Management Information Systems cybersecurity to handle expanding complex cyber threats effectively. Security measures based on traditional methods experience difficulty when dealing with both massive quantities and advanced levels of cyberattacks, which makes real-time security detection more problematic. The Big Data Analytics system provides organizations with the ability to process large security datasets, which helps identify abnormal events and security patterns related to potential threats. Using machine learning models together with predictive analytics helps Big Data Analytics boost the efficiency as well as the accuracy of security frameworks operating within the

Management Information Systems domain. The system minimizes Management Information Systems leading alarm alerts present in regular security frameworks while providing speedier responses during cybersecurity incidents. Through Big Data Analytics security solutions, organizations gain the capability to detect threats proactively, which enables them to stop and stop cyber threats from inflicting major harm. Organizations that implement Big Data Analytics in their Management Information Systems cybersecurity framework achieve regulatory compliance through superior monitoring functions extended to reporting and forensic analysis capabilities.

Future research recommendations

Blockchain systems enhance data authenticity and visibility as well as data protection because they deliver decentralized mechanisms for secure identity authentication and unalterable payment transactions and invasion. The advance of quantum computing exposes traditional encryption methods to possible breaches; therefore, Management Information Systems operators should research to develop quantum-resistant security algorithms that protect their data. The solution of these security areas helps build better, more resistant cybersecurity systems for today's information technology systems.

Figure No.04: Future Research Directions in Big Data Analytics and Cybersecurity

Acknowledgment

The research benefits from a sincere appreciation for all individuals along with organizations that helped finalize this investigation. The research received valuable input from cybersecurity professionals who conducted interviews together with Management Information Systems administrators and industry experts through surveys. The research has benefited from the support that academic institutions and research bodies provided through their access to necessary datasets and documents. The research owes much gratitude to colleagues and mentors who used their constructive ideas and knowledgeable advice to develop this research project.

References

[1] Schwieger, D., & Ladwig, C. (2022). Cyber Insurance Concepts for the Management Information Systems and Business Curriculum. *Information Systems Education Journal*, *20*(5), 54-66.

[2] Choejey, P. (2018). *Cybersecurity challenges and practices: a case study of Bhutan* (Doctoral dissertation, Murdoch University).

[3] Singh, I., & Singh, Y. A. S. H. I. K. (2022). Cyber-security knowledge and practice of nurses in private hospitals in northern Durban, KwaZulu-Natal. *Journal of Theoretical and Applied Information Technology*, *100*(1), 246-267.

[4] Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE communications surveys & tutorials*, *21*(2), 1744-1772.

[5] Kävrestad, J., & Nohlberg, M. (2021). Evaluation strategies for cybersecurity training methods: a literature review. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15* (pp. 102-112). Springer International Publishing.

[6] Benbya, H., Nan, N., Tanriverdi, H., & Yoo, Y. (2020). Complexity and information systems research in the emerging digital world. *Management Information Systems Quarterly*, *44*(1), 1-17.

[7] Al Kabir, M. A., & Elmedany, W. (2022, December). An overview of the present and future of user authentication. In *2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM)* (pp. 10-17). IEEE.

[8] Edu, Y., Eimunjeze, J., Onah, P., Adedoyin, D., David, P.O., Ikegwu, C. Fintech Update: SEC New Rules On The Issuance, Offering Platforms and Custody of Digital Assets- What You need to Know. Mondaq (July 6, 2022)

[9] Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self-optimizing and self-adaptative artificial intelligence (part 2). *Health and Technology*, *12*(5), 923-929.

[10] Younis, Y. A., Kifayat, K., Shi, Q., Matthews, E., Griffiths, G., & Lambert, R. (2020, September). Teaching cryptography using cipher (interactive cryptographic protocol teaching and learning). In *Proceedings of the 6th International Conference on Engineering & Management Information Systems 2020* (pp. 1-7).

[11] Paterson, K. G. (2021). The cyber security body of knowledge. *Version*, *1*(0), 62.

[12] Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques, and tools. In *2013 2nd national conference on Information Assurance (ncia)* (pp. 129-134). IEEE.

[13] Adebayo, A. O., Ogunbiyi, E. O., Adebayo, L. O., & Adewuyi, S. (2021). Schiff Base Modified Chitosan Iron (III) Complex as New Heterogeneous Oxidative Catalyst. Journal of Chemical Society of Nigeria, 46(2).

[14] Rassam, M. A., Maarof, M., & Zainal, A. (2017). Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. *Journal of Information Assurance & Security*, *12*(4).

[15] Eastman, R., Versace, M., & Webber, A. (2015). Big data and predictive analytics: on the cybersecurity front line. *IDC Whitepaper, February*.

[16] Soltani Delgosha, M., Hajiheydari, N. & Fahimi, S. M. Elucidation of big data analytics in banking: a four-stage Delphi study J. Enterp. Inform. Manage. 34 (6), 1577–1596 (2021).

[17] Gołębiowska, A., Jakubczak, W., Prokopowicz, D., & Jakubczak, R. (2021). Cybersecurity of business intelligence analytics is based on the processing of large sets of information with the use of sentiment analysis and Big Data. *European Research Studies Journal*, *24*(4).

[18] Pan, G., SEOW, P. S., Chan, C., & LIM, C. Y. (2015). Analytics and cybersecurity: The shape of things to come.

[19] Ahmad, F., Abidin, S., Qureshi, I., & Ishrat, M. (2022, November). Big Data and Its Role in Cybersecurity. In *International Conference on Innovations in Data Analytics* (pp. 131-144). Singapore: Springer Nature Singapore.

[20] Ali, H. (2022). AI-Powered Supervised Classifiers in Big Data Environments for Phishing Defense and Intrusion Detection.

[21] Vincent, T., & Prince, U. (2021). Implementation of critical information infrastructure protection techniques against cyber-attacks using big data analytics.

[22] Grahn, K., Westerlund, M., & Pulkkis, G. (2017). Analytics for network security: A survey and taxonomy. *Information fusion for cyber-security analytics*, 175-193.

[23] D'Alconzo, A., Drago, I., Morichetta, A., Mellia, M., & Casas, P. (2019). A survey on big data for network traffic monitoring and analysis. *IEEE Transactions on Network and Service Management*, *16*(3), 800-813.

[24] He, W., Hung, J. L. & Liu, L. Impact of big data analytics on banking: a case study. J. Enterp. Inform.

[25] Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. *Complex & Intelligent Systems*, *8*(2), 1763-1780.

[26] Himeur, Y. et al. AI-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives Artif. Intell. Rev.

[27] Javid, T., Gupta, M. K. & Gupta, A. A hybrid-security model for privacy-enhanced distributed data mining J. King Saud University-Computer Inform. Sci. 34 (6), 3602–3614 (2022).

[28] Salitin, M. A., & Zolait, A. H. (2018, November). The role of User Entity Behavior Analytics is to detect network attacks in real-time. In the *2018 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 1-5). IEEE.

[29] Tewari, S. H. (2021). Necessity of data science for enhanced cybersecurity. *International Journal of Data Science and Big Data Analytics*, *1*(1), 63-79.

[30] Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity:

[31] Mirtsch, M., Kinne, J. & Blind, K. Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. IEEE Trans. Eng. Manage. 68 (1), 87–100 (2020).

[32] Miao, Y., Ruan, Z., Pan, L., Wang, Y., Zhang, J., & Xiang, Y. (2018). Automated big traffic analytics for cyber security. *arXiv preprint arXiv:1804.09023*.

[33] Obitade, P. O. (2019). Big data analytics: a link between knowledge management capabilities and superior cyber protection. *Journal of Big Data*, *6*(1), 71.

[34] Chen, H. M., Kazman, R., & Haziyev, S. (2016, January). Agile big data analytics development: An architecture-centric approach. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5378-5387). IEEE.

[35] Singh, J. et al. Sales profession and professionals in the age of digitization and artificial intelligence technologies: concepts, priorities, and questions J. Personal Sell. Sales Manage. 39 (1), 2–22 (2019).

[36] Jiang, R., Ma, Z. & Yang, J. An assessment model for cloud service security risk based on entropy and support vector machine Concurrency Computation: Pract. Experience. 33 (21), e6423 (2021).

[37] Sommestad, T., Holm, H. & Steinvall, D. Variables influencing the effectiveness of signature-based network intrusion detection systems Inform. Secure. Journal: Global Perspective. 31 (6), 711–728 (2022).

[38] Subeesh, A. & Mehta, C. R. Automation and digitization of agriculture using artificial intelligence and internet of things Artif. Intell. Agric. 5, 278–291 (2021).

[39] Sundarakani, B., Ajaykumar, A., & Gunasekaran, A. (2021). Big data driven supply chain design and applications for blockchain: An action research using case study approach. *Omega*, *102*, 102452.

[40] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), 146.

[41] Rahman, M. S., & Reza, H. (2022). A systematic review of big data analytics in social media. *Big data mining and analytics*, *5*(3), 228-244.

[42] Zhang, Y., Huang, T., & Bompard, E. F. (2018). Big data analytics in smart grids: a review. *Energy informatics*, *1*(1), 1-24.

[43] Ahmad, A. et al. How the integration of cyber security management and incident response enables organizational learning J. Association Inform. Sci. Technol. 71 (8), 939–953 (2020).

[44] Akinola, A., & Afonja, A. (2022). *Introduction to Cyber-security*. ChudacePublishing.

[45] Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, *15*(7), 4362-4369.

[46] Maka, S. R. (2021). AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises. *Available at SSRN 5116926*.

[47] Zhu, S., Saravanan, V., & Muthu, B. (2020). Achieving data security and privacy across healthcare applications using cyber security mechanisms. *The Electronic Library*, *38*(5/6), 979-995.

[48] Richins, G., Stapleton, A., Stratopoulos, T. C., & Wong, C. (2017). Big data analytics: opportunity or threat for the accounting profession? *Journal of information systems*, *31*(3), 63-79.

[49] Ponnusamy, V. K., Kasinathan, P., Madurai Elavarasan, R., Ramanathan, V., Anandan, R. K., Subramaniam, U., ... & Hossain, E. (2021). A comprehensive review of sustainable aspects of big data analytics for the smart grid. *Sustainability*, *13*(23), 13322.

[50] Tang, B., Chen, Z., Hefferman, G., Wei, T., He, H., & Yang, Q. (2015). A hierarchical distributed fog computing architecture for big data analysis in smart cities. In *Proceedings of the ASE BigData & Social Informatics 2015* (pp. 1-6).

[51] Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of big data*, *3*, 1-25.

[52] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference* (Vol. 13, p. 13).

[53] Singh, D., & Reddy, C. K. (2015). A survey on platforms for big data analytics. *Journal of big data*, *2*, 1-20.

[54] Gupta, C. et al. A systematic review on machine learning and deep learning models for electronic information security in mobile networks Sensors, 22(5): 2017. (2022).

[55] Hirschlein, N., Meckenstock, J. N., & Dremel, C. (2022). Towards bridging the gap between BIG DATA ANALYTICS challenges and BIG DATA ANALYTICS capability: A conceptual synthesis based on a systematic literature review.

[56] Kamilaris, A., Kartakoullis, A., & Prenafeta-Boldú, F. X. (2017). A review of the practice of big data analysis in agriculture. *Computers and electronics in agriculture*, *143*, 23-37.

[57] Demchenko, Y., Grosso, P., De Laat, C., & Membrey, P. (2013, May). Addressing big data issues in scientific data infrastructure. In *2013 International conference on collaboration technologies and systems (CTS)* (pp. 48-55). IEEE.

[58] Jingle, I. D. J. & Paul, P. M. A collaborative defense protocol against collaborative attacks in wireless mesh networks[J]. Int. J. Enterp. Netw. Manage. 12 (3), 199–220 (2021).

[59] Papadopoulos, T., Gunasekaran, A., Dubey, R., Altay, N., Childe, S. J., & Fosso-Wamba, S. (2017). The role of Big Data in explaining disaster resilience in supply chains for sustainability. *Journal of cleaner production*, *142*, 1108-1118.

[60] Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, *237*, 350-361.

[61] Kabanov, I., & Madnick, S. E. (2021). Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. *MANAGEMENT INFORMATION SYSTEMS Q. Executive*, *20*(2), 4.

[62] Kim, H., & Shon, T. (2022). Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. *The Journal of Supercomputing*, *78*(11), 13554-13563.

[63] Alawadhi, S. A., Zowayed, A., Abdulla, H., Khder, M. A., & Ali, B. J. (2022, June). Impact of artificial intelligence on information security in business. In *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)* (pp. 437-442). IEEE.

[64] 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.

[65] Li, L. et al. Big data and big disaster: a mechanism of supply chain risk management in global logistics industry Int. J. Oper. Prod. Manage. 43 (2), 274–307 (2022).

[66] Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques, and tools. In *2013 2nd national conference on Information Assurance (ncia)* (pp. 129-134). IEEE.

[67] Kim, S. C., Ray, P., & Reddy, S. S. (2019). Features of smart grid technologies: an overview. *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, *17*(2), 169-180.

[68] Caramancion, K. M. (2021, October). The Role of Subject Confidence and Historical Deception in Management Information Systems/Disinformation Vulnerability. In *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0541-0546). IEEE.

[69] Spremić, M., & Šimunic, A. (2018, July). Cyber security challenges in the digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.

[70] Boehm, J., Kaplan, J. M., Merrath, P., Poppensieker, T., & Stähle, T. (2020). Enhanced cyber-risk reporting: Opening doors to risk-based cybersecurity. *McKinsey on Risk*, *9*, 1-10.

[71] Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2021). Cybersecurity challenges for software developer awareness training in industrial environments. In *Innovation Through Information Systems: Volume II: A Collection of Latest Research on Technology Issues* (pp. 370-387). Springer International Publishing.

[72] Verma, A., & Shri, C. (2022). Cyber security: A review of cybercrimes, security challenges and measures to control. *Vision*, 09722629221074760.

[73] Peres, R. S. et al. Industrial artificial intelligence in Industry 4.0-systematic review, challenges, and Outlook IEEE Access. 8, 220121–220139 (2020).

[74] Sen, R., Heim, G., & Zhu, Q. (2022). Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for Management Information Systems academics. *Communications of the Association for Information Systems*, *51*(1), 28. [75] Rassam, M. A., Maarof, M., & Zainal, A. (2017). Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. *Journal of Information Assurance & Security*, *12*(4).

[76] Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, *14*(6), 2055-2072.

[77] Leevy, J. L., & Khoshgoftaar, T. M. (2020). A survey and analysis of intrusion detection models based on cse-cic-ids2018 big data. *Journal of Big Data*, *7*, 1-19.

[78] Stergiou, C. L., Plageras, A. P., Psannis, K. E., & Gupta, B. B. (2020). Secure machine learning scenario from big data in cloud computing via the Internet of Things network. *Handbook of computer networks and cyber security: principles and paradigms*, 525-554.

[79] Sen, R., Heim, G., & Zhu, Q. (2022). Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for Management Information Systems academics. *Communications of the Association for Information Systems*, *51*(1), 28.

[80] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017, November). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In *2017 4th International Conference on Systems and Informatics (ICSAI)* (pp. 975-979). IEEE.

[81] Tavera Romero, C. A. et al. Business intelligence: business evolution after Industry 4.0Sustainability 13 (18), 10026 (2021).

[82] Amalina, F., Hashem, I. A. T., Azizul, Z. H., Fong, A. T., Firdaus, A., Imran, M., & Anuar, N. B. (2019). Blending big data analytics: Review on challenges and a recent study. *Ieee Access*, *8*, 3629-3645.

[83] Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from the neural network and deep learning perspective. *SN Computer Science*, *2*(3), 154.

[84] Chen, X. & Metawa, N. Enterprise financial management information system based on cloud computing in big data environment J. Intell. Fuzzy Syst. 39 (4), 5223–5232 (2020).

[85] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: a survey. *Journal of Big Data*, *2*, 1-41.

[86] Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.

[87] Kaffash, S., Nguyen, A. T. & Zhu, J. Big data algorithms and applications in intelligent transportation system: a review and bibliometric analysis Int. J. Prod. Econ. 231, 107868 (2021).

[88] Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MANAGEMENT INFORMATION SYSTEMS quarterly*, 1165-1188.

[89] González-Granadillo, G., González-Zarzosa, S. & Diaz, R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures Sensors 21 (14), 4759 (2021).

[90] Vadhil, F. A., Nanne, M. F. & Salihi, M. L. Importance of machine learning techniques to improve the open-source intrusion detection systems Indonesian J. Electron. Eng. Inf. (IJEEI). 9 (3), 774–783 (2021).

[91]. Yavanoglu, O., & Aydos, M. (2017, December). A review of cyber security datasets for machine learning algorithms. In *2017 IEEE international conference on big data (big data)* (pp. 2186-2193). IEEE.

[92] Kaushik, D., Garg, M., Gupta, A., & Pramanik, S. (2022). Application of machine learning and deep learning in cybersecurity: An innovative approach. In *An Interdisciplinary Approach to Modern Network Security* (pp. 89-109). CRC Press.

[93] Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big data analytics*, *1*(1), 6.

[94] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208.

[95] Tang, M., Alazab, M., & Luo, Y. (2017). Big data for cybersecurity: Vulnerability disclosure trends and dependencies. *IEEE Transactions on Big Data*, *5*(3), 317-329.

[96] Aldawsari, H., & Kouchay, S. A. Integrating AI and Machine Learning Algorithms in Cloud Security Frameworks for Enhanced Proactive Threat Detection and Mitigation.

[97] Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques, and tools. In *2013 2nd national conference on Information Assurance (ncia)* (pp. 129-134). IEEE.