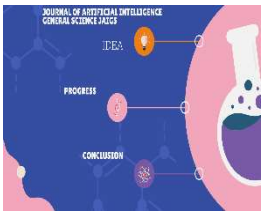
Vol.1,Issue1,January 2024
Journal of Artificial Intelligence General Science JAIGS

https://ojs.boulibrary.com/index.php/JAIGS



AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age

Hassan Rehan

Department of Computer & Information technology, Purdue University, USA.

*Corresponding Author:Hassan Rehan

ARTICLEINFO

Article History:

Received:
05.01.2024
Accepted:
10.01.2024
Online: 22.01.2024

Keyword: *AI-driven, Cloud Security, Sensitive Data, Artificial Intelligence, Machine Learning, Anomaly Detection, Threat Intelligence, Behavior Analytics, Cyber Threats, Regulatory Compliance, Ethical AI.*

ABSTRACT

As organizations increasingly rely on cloud computing for storage, processing, and deployment of sensitive data, ensuring robust security measures becomes paramount. This paper explores the intersection of artificial intelligence (AI) and cloud security, presenting AI-driven solutions as the future of safeguarding sensitive data in the digital age. Leveraging AI algorithms and machine learning techniques, cloud security can adapt and evolve to counter emerging threats in real-time, enhancing detection, prevention, and response capabilities. This paper discusses various AI-driven approaches to cloud security, including anomaly detection, threat intelligence analysis, and behavior analytics, highlighting their effectiveness in mitigating risks and ensuring compliance with regulatory standards. Additionally, it addresses the challenges and ethical considerations associated with AI-driven cloud security, emphasizing the importance of transparency, accountability, and ethical AI principles. By embracing AI-driven solutions, organizations can fortify their defenses against cyber threats and maintain the integrity and confidentiality of their sensitive data in the evolving digital landscape.

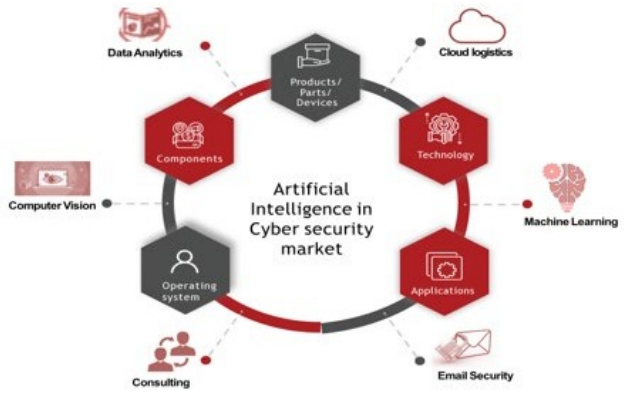
Introduction:

Cybersecurity encompasses a set of processes aimed at safeguarding electronic data, human activities, and systems. Similar to Moore's Law, which predicts the doubling of integrated circuit components every two years alongside declining costs associated with chip development, cybercriminals are rapidly enhancing the effectiveness of their targeted attacks at a fraction of the cost every few months. This exponential growth in cyber threats underscores the critical importance of cybersecurity measures.

Global spending on cybersecurity has surged, with estimates surpassing $1 trillion between 2016 and 2021. Expenditure in this domain has risen by over 40 percent from 2013 to $66, highlighting the escalating need for robust defenses against cyber threats.

Artificial Intelligence (AI) represents a significant advancement in computer systems, leveraging human-like cognitive abilities to perform tasks such as voice recognition and language processing. AI is a multidisciplinary field encompassing mathematics, computer science, and philosophy, aiming to develop intelligent systems capable of problem-solving and learning, akin to human cognition.

Machine learning plays a pivotal role in modern research and business endeavors. Through the utilization of algorithms and network-neutral models, machine learning enables computers to autonomously improve performance based on data without explicit programming. These algorithms construct mathematical models using training data to make informed decisions, mirroring the synaptic interactions within the brain cells, as conceptualized by Donald



Hebb in 1949.

Supervised Learning:

Supervised learning serves as a foundational approach in implementing machine learning algorithms, enabling pattern recognition and solution understanding. Comparable to teaching a child with flashcards, this method involves providing labeled data to train models, making it easier to comprehend solutions and widely applicable across various tools. For instance, spam classification systems in email services employ supervised learning to effectively identify and filter out unwanted emails based on labeled examples.

Unsupervised Learning:

In contrast to supervised learning, unsupervised learning operates without labeled data. Instead, it analyzes extensive datasets to uncover underlying patterns and data structures. Through pattern recognition and data clustering techniques, unsupervised learning autonomously learns to identify and categorize data without explicit guidance.

Reinforcement Learning:

Reinforcement learning diverges from both supervised and unsupervised learning paradigms. This approach involves learning through trial and error, with algorithms making decisions based on the feedback received from the environment. Commonly employed in industrial simulations and robotics, reinforcement learning enables systems to autonomously learn optimal strategies to accomplish tasks without explicit programming.

Deep Learning:

Deep learning, a subset of machine learning, facilitates automatic feature learning, allowing algorithms to extract complex features from input data. By combining multiple layers of abstraction, deep learning models can efficiently handle massive datasets and make intricate predictions. The proliferation of deep learning techniques has been instrumental in advancing fields such as cybersecurity, where complex patterns in data need to be discerned rapidly.

Genetic Algorithms and Genetic Programming:

Genetic algorithms (GA) and genetic programming (GP) are computational methods inspired by the principles of evolution. These algorithms operate on populations of potential solutions, evolving them over successive generations through selection, crossover, and mutation operators. By iteratively improving the fitness of individuals within the population, genetic algorithms and genetic programming can efficiently search solution spaces and optimize complex problems.

Application in Cybersecurity:

These machine learning algorithms find extensive application in cybersecurity, where the detection of cyber threats and attacks is crucial. Researchers utilize various ML techniques, including supervised, unsupervised, and reinforcement learning, to develop models capable of identifying and mitigating cyber-attacks. For instance, evaluating the effectiveness of ML algorithms in detecting cyber-attacks on MODBUS data involves techniques such as tenfold cross-validation, which enables the robust assessment of model performance using labeled telemetry data from critical infrastructure systems like gas pipelines.

Cloud Computing-based Machine Learning Systems for Cybersecurity:

Bhamare et al. (2016) investigated the evolution of Industrial Control Systems (ICS) from autonomous setups to cloud-based environments. They surveyed prominent works from both industry and academia concerning the development of secure ICS, particularly focusing on the application of machine learning techniques for cybersecurity in ICS. Their research aims to tackle the challenges associated with securing industrial processes, especially during their migration to cloud infrastructures. Additionally, Rassam et al. (Year) highlighted the escalating sophistication of cybercriminal tactics, emphasizing the importance of collecting comprehensive security data for forensic analysis. However, handling large-scale data and minimizing false alarms, especially within cloud architectures, poses significant challenges. The authors underscored the need for accurate and swift analysis of vast

security datasets to detect emerging threats like Advanced Persistent Threats (APTs). They explored the utilization of big data processing techniques in various domains and discussed vulnerabilities in traditional technologies and Security Information and Event Management (SIEM) tools. Furthermore, they outlined criteria for advanced data analytics and the identification of sophisticated cyber threats, alongside addressing the challenges and suggesting future research directions for enhancing cybersecurity adoption.

Moreover, the integration of cloud-based applications has revolutionized numerous business models, particularly in the financial sector, with emerging technologies like big data and cloud computing. However, this paradigm shift has also amplified concerns regarding cybersecurity, leading to the growth of the cyber insurance industry. The article delves into the intricate taxonomy of cybersecurity risks, coupled with machine learning techniques, to mitigate potential threats effectively.

Furthermore, technological advancements such as the Internet of Things (IoT), cloud computing, smartphones, and social networks have ushered in new cyber threats, necessitating innovative approaches to cybersecurity. Cognitive science is proposed as a solution to augment the capabilities of security analysts in handling complex cyber threats by providing comprehensive machine learning and decision-making systems. This model facilitates information dissemination, understanding, and prompt response to security incidents, incorporating automation techniques and cognitive processes in cyber operations.

Additionally, the manufacturing sector is undergoing a transformation with the integration of technologies like the Industrial Internet of Things (IIoT), big data analytics, cloud computing, and advanced robotics. However, the increased connectivity and digitization also expose manufacturing systems to cyber threats. Anqi Re et al. (Year) explored cutting-edge technologies to address cybersecurity challenges in intelligent production systems, emphasizing vulnerability assessment, cyber attack mitigation strategies, and research gaps in critical manufacturing industries.

In conclusion, the convergence of cloud computing and machine learning holds immense potential for bolstering cybersecurity measures across various domains, from industrial control systems to intelligent manufacturing. However, it also necessitates proactive measures to address evolving cyber threats and vulnerabilities inherent in digital transformations like Industry 4.0.

Organizational Risk Assessment of Cybersecurity using AI:

Nishant et al. (Year) emphasized the need for AI to foster organizational processes and practices that align with cultural norms, aiming to minimize the ecological footprint of human activities while promoting innovation in environmental sustainability solutions. Their research highlighted concerns regarding the over-reliance on historical data in machine learning models, unpredictable human responses to AI interventions, increased cyber risks, adverse AI implementations, and challenges in measuring the impacts of intervention policies on sustainability. They suggested future sustainable AI studies incorporate multi-level perspectives, dynamic system approaches, design thinking, and economic benefit considerations to offer immediate solutions without compromising long-term environmental sustainability.

Moreover, Soni et al. (Year) conducted an extensive analysis of the broad-ranging impacts of Artificial Intelligence (AI) on governments, counties, companies, and individuals, assessing both positive and negative consequences. Their study explored the trajectory of AI from research and development to implementation, examining its academic achievements, influence on business practices, and global market dynamics. Additionally, they identified factors driving AI development and analyzed entrepreneurial activities in the AI sector, providing insights into technological advancements and their societal and economic implications.

Furthermore, Haque et al. (Year) conducted a bibliometric analysis of studies focusing on big data and AI technologies in the maritime industry. Their research analyzed 279 studies authored by 842 scholars across 214 university outlets, identifying influential journals, authors, and research clusters such as AI applications in big data, energy efficiency, predictive analysis, and digital transformation in the maritime sector. They also examined research partnership networks and institutional collaborations to facilitate knowledge exchange and identify potential areas for further study.

Lastly, Tagarev et al. (Year) highlighted the imperative of digital transformation to bolster cybersecurity in critical infrastructures and essential services. Their volume, comprising 28 papers presented at the DIGILIENCE 2019 conference, addressed themes such as cyber information sharing, emerging technologies like AI, the human factor in cybersecurity, education and training, and cyber resilience. The DIGILIENCE Conference series serves as a platform for exchanging information and expertise in IT management, cybersecurity, and resilience, facilitating the dissemination of best practices to enhance cyber safety efforts.

Blockchain Technology Utilizing AI:

The utilization of blockchain technology extends beyond its traditional applications in accounting and cybersecurity, as explored by researchers [25]. Authors delve into both existing and potential future business applications of blockchain, particularly in addressing cybersecurity and accounting challenges. By examining literature encompassing topics such as the handling of large-scale data in accounting, financial security, cyber security, and the utilization of ledger technology in financial accounts, researchers aim to identify opportunities for blockchain implementation.

Furthermore, researchers analyze the implications of blockchain technology on auditing practices, anticipating significant changes in the profession. They also consider the U.S. government's cybersecurity policy, particularly initiatives outlined by the Department of Homeland Security, to gain insights into future cybersecurity strategies. Highlighting the diverse auditing implications of blockchain, researchers emphasize the need for effective implementation across various domains, including auditing, accounting, and cybersecurity, to harness its transformative potential fully.

IoT-Based Cyberattack Prevention Systems:

Ioanni et al. (Year) conducted an extensive examination of IoT-enabled cyberattacks spanning various application domains since 2010. They meticulously analyzed recent attacks, globally renowned incidents, and proof-of-concept attacks across sectors. Through methodical analysis, the authors identified direct and indirect pathways through which critical targets are vulnerable to cyber threats. Their research aims to achieve three objectives: first, to present a risk assessment landscape for IoT-enabled cyberattacks; second, to identify overwhelmed and subtle attack pathways targeting critical infrastructure and services; and third, to propose mitigation strategies across different application areas.

Furthermore, the integration of Artificial Intelligence (AI) with the Internet of Things (IoT) has paved the way for enhanced cybersecurity measures. Researchers (Year) provided insights into the convergence of IoT and AI, exploring AI algorithms, challenges, and systems. They emphasized the significance of self-optimizing networks and software-defined networks within major IoT system parameters, enabling efficient data processing and storage across IoT networks.

Moreover, the proliferation of IoT has led to significant advancements in various domains such as smart homes, intelligent transportation, and healthcare. However, it has also introduced new cybersecurity challenges. Authors (Year) discussed emerging cybersecurity threats and opportunities for research and innovation in the context of "Cyber Security + Edge Computing + IoT + AI." They highlighted the need for addressing cybersecurity concerns in tandem with the advancement of IoT technologies.

Additionally, Monika et al. (Year) delved into the application of deep learning models in IoT networks for cybersecurity. They addressed the pressing need for robust cybersecurity measures in rapidly expanding IoT deployments. By proposing and testing deep learning models using advanced datasets, they demonstrated promising results in detecting Distributed Denial of Service (DDoS) attacks. Their research also identified open research issues for further exploration in IoT cybersecurity.

Furthermore, the development of cybersecurity frameworks powered by data analysis has gained traction in recent years. In a paper by authors (Year), a security operations framework combining traditional data processing layers with modern analytical database engines was presented. This framework enables security experts to query large log event datasets effectively, facilitating the identification of suspicious activities. The paper analyzed the impact of various engine parameters on efficiency and discussed high-level design decisions.

Moreover, authors (Year) proposed an approach to cybersecurity science driven by data (SOS), emphasizing evidence-based science, confidence and policy-based mechanisms for information sharing, and risk-based security approaches. They argued that these aspects form the foundation for advancing the science of cybersecurity.

Lastly, authors (Year) developed models for discrete event simulation to evaluate the impact of unintended attacks on device security. By considering parameters such as user vulnerability and interactions, they assessed the potential effects of such attacks on system health. Their simulation model enables comprehensive analyses of system vulnerabilities and provides insights for enhancing cybersecurity strategies.

In conclusion, the integration of IoT with advanced technologies such as AI and data analysis presents opportunities for enhancing cybersecurity measures, but also introduces new challenges that require innovative solutions and robust frameworks.

Involvement of AI in Intrusion Detection Systems (IDS):

Xavier et al. (Year) proposed algorithms for learning systems tailored specifically for Intrusion Detection Systems (IDS). Their approach involved categorizing cybersecurity datasets into multiple groups to optimize model selection within neural networks, considering factors such as network architecture (multilayer or recurrent), activation functions, and learning algorithms. By analyzing the results, they identified key data categories crucial for intrusion detection and determined the most suitable machine learning configurations to minimize computational burden. Additionally, the authors addressed significant safety risks associated with interconnected systems essential for advanced features in automobiles, drawing parallels between their IDS approach and the concepts applied in self-driving car systems.

Similarly, Iqbal et al. (Year) presented a safety-oriented machine learning model based on the IntruD Tree method, which prioritizes safety feature ratings to construct an overarching tree-based intrusion detection model. This model not only demonstrates predictive accuracy for various test cases but also reduces model complexity by minimizing feature dimensions. The effectiveness of the IntruD Tree model was evaluated using cybersecurity datasets, measuring precision, accuracy, and Receiver Operating Characteristic (ROC) values. Comparative analysis against traditional machine learning approaches, such as naive Bayes, logistic regression, support vector machines, and k-nearest neighbors, was conducted to assess the efficacy of the proposed safety model.

Furthermore, a neuromorphic cognitive computing approach for Deep Learning (DL)-based Cybersecurity Network Intrusion Detection System (IDS) was proposed in a study by authors (Year). This innovative approach combined the algorithmic power of DL with fast and highly efficient neuromorphic cybersecurity processors. The training process involved encoding data using an autoencoder and discrete factorization of vectors, followed by mapping the generated weights into crossbars and neurons. Test results using the IBM Neurosynaptic Core Simulator (NSCS) and the neurosynaptic TrueNorth chip demonstrated an impressive accuracy of approximately 90.12% for cyber security intrusion detection. Additionally, the framework was capable of classifying various types of attacks with a precision of 81.31%, showcasing its effectiveness in detecting and categorizing network intrusions.

Lastly, machine learning technology has found widespread application in cybersecurity, particularly in areas such as malware analysis, threat detection, and intrusion anomaly detection. In a study by authors (Year), machine learning techniques were discussed as efficient alternatives to signature-based approaches for detecting zero-day malware and analyzing threats. The research also addressed challenges associated with adversarial attacks on machine learning algorithms, highlighting the need for robust methodologies in cybersecurity applications.

Software Defined Networks (SDNs) Attacks and AI:

The intersection of software vulnerabilities, internet susceptibility, and the burgeoning accumulation of unprocessed data in big data frameworks poses significant challenges in the realm of computing. These issues, rooted in human intervention, necessitate novel solutions that transcend traditional approaches. In a study by (Author et al., Year), a paradigm shift towards the complete elimination of human intervention is proposed. This radical yet theoretical approach conceptualizes the cause set—a mathematical construct—as the universal language underlying all information and computation. By relying solely on the cause set and its metric, alongside its extensive array of algebraic properties, this novel theory offers unforeseen and groundbreaking outcomes. The proposed framework advocates for the confinement of languages to the human interface, with an inner layer of mathematically verified code expressed as a causal set, ensuring that machines interact solely with bug-free and secure code. The paper encompasses experimental and computational validations, outlining potential applications in internet vulnerability

mitigation, science, technology, machine learning, computer intelligence, and detailed instructions for prototype development.

Carla Saya et al. (Year) delve into the design and implementation of an Intelligent Cybersecurity Assistant (ICSA) architecture, aimed at providing expert support for cybersecurity analysts. Focusing on the rapid proliferation of malicious cyber events and their impact on normal cyber operations, the study emphasizes the necessity for advanced machine learning techniques to autonomously detect and thwart cyber-attacks. The proposed ICSA system leverages smart cyber assistant technology to efficiently defend against both existing and emerging threats. Through adaptive learning capabilities, the ICSA enhances intelligence collection and analysis, enabling the swift identification and mitigation of vulnerabilities.

In another study (Author et al., Year), a framework utilizing Semantic Web technologies is introduced to enhance cybersecurity measures. This framework facilitates the automatic extraction and analysis of text from online sources, enabling cyber security experts to detect malicious activities perpetrated by black hat hackers. By analyzing various internet networks and communication patterns of hacking groups, the framework aims to provide valuable insights into potential cyber threats. The model processes natural language cybersecurity-related data to gather actionable information for further analysis by experts, paving the way for future software system implementations.

As technological advancements continue to reshape the landscape, the need for cybersecurity education becomes increasingly imperative. (Author et al., Year) embarked on a research endeavor aimed at fostering interest and awareness of cybersecurity across all age groups. Through an innovative approach, the study sought to gamify cybersecurity education to make it more engaging and accessible. Participants engaged in surveys and self-assessments to evaluate the effectiveness of the new educational system, with the study concluding with an analysis of the survey results and potential refinements to enhance its efficacy.

Prevention of Cyber-Attacks and Threats using AI:

Artificial intelligence represents a computerized iteration of human intelligence, functioning iteratively akin to human learning processes. As the threat landscape continues to evolve rapidly in this century, traditional methods of cybersecurity are proving inadequate against cyber attackers driven solely by financial incentives. Recognizing the need for innovative approaches, (Author et al., Year) emphasize the importance of developing cybersecurity skills and leveraging artificial neural networks and machine learning algorithms to enhance defense mechanisms. The paper provides an overview of social engineering, its role in networking and cyber identity theft, and its impact on cybercrimes. Additionally, it suggests preventive actions and potential solutions to mitigate threats and vulnerabilities associated with social engineering attacks. While acknowledging the role of technology in mitigating social engineering attacks, the authors emphasize that vulnerabilities primarily stem from human behavior, mental impulses, and psychological predispositions. They advocate for investments in organizational education initiatives targeting social engineering sensitivities to effectively reduce such attacks.

The proliferation of cybercrime, resulting in substantial financial losses and compromised security, underscores the critical importance of computer system security measures. In response, (Author et al., Year) discuss recent

advancements in utilizing cybersecurity datasets for assessing intrusion detection systems based on machine learning and data mining techniques. They highlight the inadequacy of existing benchmark standards for cybersecurity datasets, such as KDD and UNM, due to their failure to align with current developments in computer technology. Proposing a new benchmark dataset, ADFA Linux dataset (ADFA-LD), the authors aim to address this gap by offering better-defined attributes and aligning with contemporary advancements in global computer technology. The introduction of ADFA-LD is expected to facilitate more effective evaluations of computer and data mining intrusion detection systems within the research community.

Social and internet traffic analysis plays a crucial role in identifying and defending against cyber threats, with automated machine learning approaches increasingly replacing traditional rule-based methods. (Author et al., Year) conduct an analytical study of cyber traffic through social networking and the internet, employing data-driven models to analyze common similarity, relational, and collective indicators. This data-driven approach to internet security encompasses data collection, cyber security engineering, and cyber security modeling, aiming to enhance situational awareness and defense capabilities. Despite its potential, challenges and future directions in data-driven cyber security are also discussed.

The United States faces significant national security threats from cyber-attacks, necessitating proactive measures to deter and mitigate potential attacks. (Author et al., Year) introduce the AZ Safe Hacker Assets Portal, a proactive cyber threat intelligence (CTI) platform that gathers and analyzes malicious artifacts from online hacker groups using state-of-the-art machine learning techniques. By tapping into previously untapped data sources, such as online hacker forums, the portal aims to provide timely insights and analysis to enhance cyber threat intelligence and defense strategies.

In response to the escalating complexity of cyber threats, experts are increasingly turning to artificial intelligence (AI) to bolster cybersecurity measures. (Author et al., Year) offer a brief survey and insights on Bayesian cyber security applications, enabling quantitative threat assessment for risk analysis and situational awareness. Additionally, (Author et al., Year) provide a comprehensive survey of works on cyber security machine learning (ML), covering popular ML algorithms and proposed ML schemes for feature extraction, dimension reduction, classification, and detection. The article also addresses adversary ML and outlines potential future avenues for research and development in cybersecurity.

Business-based Cybersecurity and AI Involvement:

Narcisa Roxana et al. [13] underscore the advantages of leveraging Artificial Intelligence (AI) to enhance business competitiveness while addressing concerns surrounding emerging technologies and cyber-attacks. They emphasize the ubiquitous vulnerability of computerized systems to cyber threats and propose utilizing cyber protection strategies to safeguard businesses, with insights drawn from risk management cases in Malta. The article delves into the current state of AI in cybersecurity, presenting various case studies and applications to elucidate unresolved issues and challenges. Furthermore, it offers implications for business and government management, along with policy recommendations.

In the rapidly evolving landscape of cybersecurity, data science plays a pivotal role in driving progress and innovation. (Author et al., Year) focus on the application of data science methodologies to enhance cybersecurity by automating security architecture and deriving actionable insights from cybersecurity data. By leveraging machine learning techniques and data-driven models, the paper aims to make cybersecurity operations more efficient and intelligent. It addresses key research problems and offers recommendations for advancing cybersecurity data science, culminating in a multi-layered machine learning framework for cybersecurity modeling.

Digital advancements have transformed supply chain processes, posing new challenges and risks related to cybersecurity. Through a systematic literature review, (Author et al., Year) examine the impact of disruptive technologies on supply chains and the associated cyber threats. They employ a taxonomy approach to evaluate progress, particularly in mitigating cyber risks within the context of Industrial Internet of Things (IIoT) and Industry 4.0. The paper describes an autonomous AI/ML and Real-Time Intelligence system designed to support supply chain infrastructure for predictive cyber risk analysis. This system, integrated with IoT networks, enhances capabilities and provides insights into deploying edge computing nodes while addressing associated risks.

Medical Image Processing and Cyber Attacks:

Miles et al. [54] highlight the unprecedented growth of machine learning and artificial intelligence (AI), which find various applications ranging from machine translation to medical image processing. While these technologies offer numerous benefits, the potential for their misuse has historically received less attention. The report delves into the landscape of potential safety risks stemming from the misuse of AI technologies and proposes strategies to predict, prevent, and mitigate them. The authors analyze the long-term equilibrium between aggressors and defenders, emphasizing the importance of developing adequate protection to anticipate and counteract emerging threats.

Advancements in Cryptographic and Artificial Intelligence Techniques:

Cybersecurity is a dynamic field that has garnered significant attention over the past decade due to the escalating number of threats and the evolving tactics of cybercriminals. While the underlying motivations for cyber-attacks have remained relatively consistent, cybercriminals are continuously enhancing their methodologies, rendering traditional cybersecurity solutions less effective in detecting and mitigating new threats. However, advancements in cryptographic and artificial intelligence (AI) techniques, particularly in machine learning and deep learning, offer promising avenues for cybersecurity experts to counter the ever-growing threat landscape posed by adversaries.

In their work [55], the authors explore the potential of AI to enhance cybersecurity solutions, acknowledging both its strengths and limitations. They discuss various research opportunities within the cybersecurity domain related to the advancement of AI techniques across diverse application domains. Additionally, Faezeh et al. [56] propose an intelligent-classic hybrid restoration and compensation solution for cyber-attacks targeting Cyber-Physical Systems (CPS) and industrial Internet of Things (IoT) devices via shared communication networks. Their approach involves deploying a smart classical control system coupled with neural networks to mitigate cyber-attacks and ensure device stability in monitoring applications.

As cybercrimes continue to pose significant threats amid unprecedented advancements in information technology (IT), there is a growing need for highly efficient defense systems that are scalable, adaptable, and resilient. Modern artificial intelligence tools have emerged as crucial assets in identifying and preventing cybercrime. The study [10] aims to showcase progress in combating various cybercrimes using artificial intelligence and demonstrate the effectiveness of different AI techniques in detecting and preventing cyber-attacks. While AI can significantly enhance the detection rates of Intrusion Detection and Prevention Systems (IDPS) and aid in mining botnet source

data, its application also introduces new risks that cybersecurity experts must carefully balance against potential benefits.

Wireless Communication-Based Cyberattacks and AI-Enabled Prevention:

With the emergence of wireless communication networks, including technologies like self-driving automobiles, unmanned air systems, and the Internet of Things (IoT), there's a growing demand for high data speeds, low latencies, and reliability, particularly with the advent of the 5th generation of wireless networks (5G). Many experts argue that the integration of artificial intelligence (AI) is essential for the success of 5G wireless networks, as they generate vast amounts of data, requiring predictive analytics and efficient cell designs to meet user demands. In their work [58], the authors provide an extensive analysis of AI applications in 5G wireless networks, aiming to examine its role, analyze case studies, address challenges, and offer recommendations for future testing in 5G wireless communications.

As cyberspace becomes increasingly integral to modern life, the dependence on the internet has escalated, thereby exposing users to a myriad of cyber threats. In response, cybersecurity has become paramount in combating cyber threats, attacks, and fraud. In a survey [59], authors provide an overview of various machine learning (ML) techniques employed in cybersecurity, focusing on detection methods for potential cyber threats. They review the current literature on ML models for cybersecurity applications and compare the time complexity of widely used ML models. Additionally, the study evaluates the performance of different classifiers based on commonly used datasets and cyber threat sub-domains.

The creation of a cyber-security testing system testbed using Supervisory Control and Data Acquisition (SCADA) is proposed in [60]. The testbed involves subjecting a water storage tank control device to comprehensive cyber-attacks to collect network traffic data for training machine learning algorithms. Results demonstrate the effectiveness of ML models in real-time attack detection within SCADA settings.

Moreover, research [61] delves into artificial intelligence and cognitive dynamic systems, discussing their structures and implementation in cybersecurity. Additionally, the integration of knowledge graphs and cybersecurity is explored in [62], where a cybersecurity knowledge base is developed using ontology and machine learning techniques for attack identification and rule deduction.

Lastly, recent advancements in artificial intelligence (AI) are poised to revolutionize military power, geopolitical competition, and global politics. The paper [63] identifies AI innovations with significant implications for military applications, from tactical to strategic levels, emphasizing the need to address uncertainties and vulnerabilities posed by rapid AI growth.

Deep Learning-Based Cybersecurity Systems:

In their work [64], V. Kanimozhi et al. proposed a framework leveraging artificial neural networks that achieved an exceptional accuracy score of 99.97% and an average area under the Receiver Operator Characteristic (ROC) curve

of 0.999, with a negligible False Positive average of 0.001. The system, employing artificial intelligence for botnet attack detection, demonstrates high efficiency, precision, and effectiveness. The proposed framework, tailored for standard network traffic analysis, cyber-physical system traffic data, and real-time network traffic analysis, holds promise for implementation across various devices.

As cyber threats evolve in sophistication, conventional detection techniques face challenges in distinguishing malicious activities from benign ones, leading to high false positive rates. In response, [65] proposes leveraging automated detection techniques to respond to unfavorable user actions automatically, enhancing system protection. Comparing Q-learning with a typical stochastic game, the study suggests promising possibilities for Naive Q-Learning, even in scenarios with minimal knowledge about opponents' strategies.

Furthermore, the integration of artificial intelligence (AI) in the public sector presents numerous opportunities and challenges. Research in [66] identifies ten fields for AI applications in the public sector, delineating their development values and illustrating specific cases of public usage. Additionally, four main dimensions of AI challenges are outlined, accompanied by theoretical and practical implications, along with recommendations for future research.

A focus on deep learning (DL) approaches in cybersecurity, including intrusion detection, malware detection, phishing/spam detection, and website default detection, is provided by Samaneh et al. [69]. The study offers preliminary descriptions of common DL models and algorithms, proposing a general DL architecture for cyber security applications. Meanwhile, Yang Lu et al. [70] offer a comprehensive survey of AI and deep learning from 1961 to 2018, providing a valuable guide through the multifaceted analysis of AI applications, algorithms, and potential developments.

Moreover, Benoit et al. [71] advocate for the development of new AI techniques tailored for cybersecurity applications, emphasizing the use of KNS, probabilistic reasoning, and Bayesian updates to enhance security measures. Additionally, emerging technologies such as homomorphic encryption, blockchain, and quantum computing are explored for their impact on cyber defense and attack capabilities in [7], offering insights into potential positive and negative effects on cyber security.

Addressing the growing demand for AI expertise in academia, research [72] introduces a notebook titled "A Trellis for Novice AI Practitioners," designed to familiarize computer science and cybersecurity students with AI concepts and capabilities. The notebook facilitates hands-on experience in intrusion detection data, aiding in mitigating common cyber vulnerabilities and promoting curriculum planning for AI technologies in cybersecurity education.

AI-Driven Cybersecurity:

In their work [73], Jiageng et al. provide a comprehensive exploration of "AI-driven cyber security," emphasizing its pivotal role in intelligent cyber security services and management. Utilizing AI approaches for threat intelligence

modeling promises to streamline and enhance the cybersecurity process compared to traditional security systems. The paper also outlines various research directions to guide future investigations in the field, serving as a valuable reference and guidance for cyber security researchers and practitioners, particularly from a smart computer or technological perspective grounded in AI principles.

Describing the ontology of the reachability matrix (RMO), Noemi et al. [74] introduce a novel approach to defining networks and the cyber security domain for calculating information on accessibility. The RMO precisely determines the reachability between network nodes, incorporating elements of network structure, accessibility details, and access control policies. Additionally, the paper outlines the use of SWRL rules and SPARQL queries to refine the calculation of the Reachability Matrix, presenting an innovative methodology for reachability matrix computation.

The integration of artificial intelligence (AI) into cybersecurity holds immense potential, as highlighted in the research paper [75], which evaluates emerging issues related to artificial cyber security intelligence in the United States. Proposing a groundbreaking Artificial Intelligence Cyber Security approach, the paper underscores the rapid advancements in AI technology and its diverse applications, from face recognition to image processing. While AI technology enhances cyber security tools, it also poses challenges as malicious actors may exploit new opportunities. Consequently, the paper offers insights into leveraging artificial intelligence for both offensive and defensive cyber security strategies.

Conclusion:

As cybercrimes continue to evolve in complexity, there is an urgent need for cyber security strategies to become more resilient and intelligent. This shift will enable defense mechanisms to make timely and effective decisions in response to sophisticated attacks. To facilitate this advancement, researchers and practitioners must familiarize themselves with existing cyber security methodologies, particularly those leveraging artificial intelligence (AI) in the fight against cybercrimes.

However, despite the growing importance of AI in combating cybercrimes, there remains a lack of comprehensive summaries regarding its application in this domain. In this context, the papers reviewed in "The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey" were analyzed using both quantitative and qualitative approaches through systematic mapping across various fields, including IoT, Blockchain, Cybercrimes, Business, IDS, Software-defined networks, and cyber forensics.

The analysis revealed that artificial intelligence methodologies have made significant contributions to cyber security, particularly in enhancing intrusion detection systems. Notably, these approaches have led to reductions in computational complexity, model training times, and false alarms. However, it is essential to note that the research landscape is somewhat skewed, with a predominant focus on intrusion detection and prevention systems. Among the techniques employed, support vector machines emerged as the most dominant approach.

In conclusion, while artificial intelligence holds tremendous potential in bolstering cyber security efforts, there is a need for further research and exploration across a broader spectrum of cyber security domains. By continuing to advance AI-driven solutions and addressing existing challenges, the cyber security community can better equip itself to combat emerging cyber threats effectively.

References:

[1]. Guzman, N. (2023). Advancing NSFW Detection in AI: Training Models to Detect Drawings, Animations, and Assess Degrees of Sexiness. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 275-294. DOI: https://doi.org/10.60087/jklst.vol2.n2.p294

[2]. Kumar, B. K., Majumdar, A., Ismail, S. A., Dixit, R. R., Wahab, H., & Ahsan, M. H. (2023, November). Predictive Classification of Covid-19: Assessing the Impact of Digital Technologies. In *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1083-1091). IEEE. Doi:https://doi.org/10.1109/TNNLS.2011.2179810

[3]. Schumaker, R. P., Veronin, M. A., Rohm, T., Boyett, M., & Dixit, R. R. (2021). A data driven approach to profile potential SARS-CoV-2 drug interactions using TylerADE. *Journal of International Technology and Information Management*, *30*(3), 108-142. DOI: https://doi.org/10.58729/1941-6679.1504

[4]. Schumaker, R., Veronin, M., Rohm, T., Dixit, R., Aljawarneh, S., & Lara, J. (2021). An Analysis of Covid-19 Vaccine Allergic Reactions. *Journal of International Technology and Information Management*, *30*(4), 24-40. DOI: https://doi.org/10.58729/1941-6679.1521

[5]. Dixit, R. R., Schumaker, R. P., &Veronin, M. A. (2018). A Decision Tree Analysis of Opioid and Prescription Drug Interactions Leading to Death Using the FAERS Database. In *IIMA/ICITED Joint Conference 2018* (pp. 67-67). INTERNATIONAL INFORMATION MANAGEMENT ASSOCIATION. https://doi.org/10.17613/1q3s-cc46

[6]. Veronin, M. A., Schumaker, R. P., Dixit, R. R., &Elath, H. (2019). Opioids and frequency counts in the US Food and Drug Administration Adverse Event Reporting System (FAERS) database: A quantitative view of the epidemic. *Drug, Healthcare and Patient Safety*, 65-70. https://www.tandfonline.com/doi/full/10.2147/DHPS.S214771

[7]. Veronin, M. A., Schumaker, R. P., & Dixit, R. (2020). The irony of MedWatch and the FAERS database: an assessment of data input errors and potential consequences. *Journal of Pharmacy Technology*, *36*(4), 164-167.

https://doi.org/10.1177/8755122520928

[8]. Veronin, M. A., Schumaker, R. P., Dixit, R. R., Dhake, P., &Ogwo, M. (2020). A systematic approach to'cleaning'of drug name records data in the FAERS database: a case report. *International Journal of Big Data Management*, *1*(2), 105-118. https://doi.org/10.1504/IJBDM.2020.112404

[9]. Schumaker, R. P., Veronin, M. A., & Dixit, R. R. (2022). Determining Mortality Likelihood of Opioid Drug Combinations using Decision Tree Analysis. https://doi.org/10.21203/rs.3.rs-2340823/v1

[10]. Schumaker, R. P., Veronin, M. A., Dixit, R. R., Dhake, P., & Manson, D. (2017). Calculating a Severity Score of an Adverse Drug Event Using Machine Learning on the FAERS Database. In *IIMA/ICITED UWS Joint Conference* (pp. 20-30). INTERNATIONAL INFORMATION MANAGEMENT ASSOCIATION.

[11]. Dixit, R. R. (2018). Factors Influencing Healthtech Literacy: An Empirical Analysis of Socioeconomic, Demographic, Technological, and Health-Related Variables. *Applied Research in Artificial Intelligence and Cloud Computing*, *1*(1), 23-37.

[12]. Dixit, R. R. (2022). Predicting Fetal Health using Cardiotocograms: A Machine Learning Approach. *Journal of Advanced Analytics in Healthcare Management*, *6*(1), 43-57. Retrieved from https://research.tensorgate.org/index.php/JAAHM/article/view/38

[13]. Dixit, R. R. (2021). Risk Assessment for Hospital Readmissions: Insights from Machine Learning Algorithms. *Sage Science Review of Applied Machine Learning*, *4*(2), 1-15. Retrieved from https://journals.sagescience.org/index.php/ssraml/article/view/68

[14]. Ravi, K. C., Dixit, R. R., Singh, S., Gopatoti, A., & Yadav, A. S. (2023, November). AI-Powered Pancreas Navigator: Delving into the Depths of Early Pancreatic Cancer Diagnosis using Advanced Deep Learning Techniques. In *2023 9th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSS58085.2023.10407836

[15]. Khan, M. S., Dixit, R. R., Majumdar, A., Koti, V. M., Bhushan, S., & Yadav, V. (2023, November). Improving Multi-Organ Cancer Diagnosis through a Machine Learning Ensemble Approach. In *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1075-1082). IEEE. https://doi.org/10.1109/ICECA58529.2023.10394923

[16]. Ramírez, J. G. C. (2023). Incorporating Information Architecture (ia), Enterprise Engineering (ee) and Artificial Intelligence (ai) to Improve Business Plans for Small Businesses in the United States. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(1), 115-127. **DOI:** https://doi.org/10.60087/jklst.vol2.n1.p127

[17]. Ramírez, J. G. C. (2024). AI in Healthcare: Revolutionizing Patient Care with Predictive Analytics and Decision Support Systems. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 31-37. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p37

[18]. Ramírez, J. G. C. (2024). Natural Language Processing Advancements: Breaking Barriers in Human-Computer Interaction. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 31-39.**DOI:** https://doi.org/10.60087/jaigs.v3i1.63

[19]. Ramírez, J. G. C., &mafiqul Islam, M. (2024). Application of Artificial Intelligence in Practical Scenarios. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19. **DOI:** https://doi.org/10.60087/jaigs.v2i1.41

[20]. Ramírez, J. G. C., & Islam, M. M. (2024). Utilizing Artificial Intelligence in Real-World Applications. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19.

DOI: https://doi.org/10.60087/jaigs.v2i1.p19

[21]. Ramírez, J. G. C., Islam, M. M., & Even, A. I. H. (2024). Machine Learning Applications in Healthcare: Current Trends and Future Prospects. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1).**DOI:** https://doi.org/10.60087/jaigs.v1i1.33

[22]. RAMIREZ, J. G. C. (2023). How Mobile Applications can improve Small Business Development. *Eigenpub Review of Science and Technology*, *7*(1), 291-305.**https://studies.eigenpub.com/index.php/erst/article/view/55**

[23]. RAMIREZ, J. G. C. (2023). From Autonomy to Accountability: Envisioning AI's Legal Personhood. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(9), 1-16.https://researchberg.com/index.php/araic/article/view/183

[24]. Ramírez, J. G. C., Hassan, M., & Kamal, M. (2022). Applications of Artificial Intelligence Models for Computational Flow Dynamics and Droplet Microfluidics. *Journal of Sustainable Technologies and Infrastructure Planning*, *6*(12).https://publications.dlpress.org/index.php/JSTIP/article/view/70

[25]. Ramírez, J. G. C. (2022). Struggling Small Business in the US. The next challenge to economic recovery. *International Journal of Business Intelligence and Big Data Analytics*, *5*(1), 81-91.https://research.tensorgate.org/index.php/IJBIBDA/article/view/99

[26]. Ramírez, J. G. C. (2021). Vibration Analysis with AI: Physics-Informed Neural Network Approach for Vortex-Induced Vibration. *International Journal of Responsible Artificial Intelligence*, *11*(3).https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/77

[27]. Shuford, J. (2024). Interdisciplinary Perspectives: Fusing Artificial Intelligence with Environmental Science for Sustainable Solutions. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 1-12.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p12

[28]. Islam, M. M. (2024). Exploring Ethical Dimensions in AI: Navigating Bias and Fairness in the Field. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 13-17.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p18

[29]. Khan, M. R. (2024). Advances in Architectures for Deep Learning: A Thorough Examination of Present Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 24-30. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p30

[30]. Shuford, J., & Islam, M. M. (2024). Exploring the Latest Trends in Artificial Intelligence Technology: A Comprehensive Review. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1). **DOI:** https://doi.org/10.60087/jaigs.v2i1.p13

[31]. Islam, M. M. (2024). Exploring the Applications of Artificial Intelligence across Various Industries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 20-25.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p25

[32]. Akter, S. (2024). Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 25-30.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p30

[33]. Rana, S. (2024). Exploring the Advancements and Ramifications of Artificial Intelligence. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 30-35.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p35

[34]. Sarker, M. (2024). Revolutionizing Healthcare: The Role of Machine Learning in the Health Sector. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 35-48.

DOI: https://doi.org/10.60087/jaigs.v2i1.p47

[35]. Akter, S. (2024). Harnessing Technology for Environmental Sustainability: Utilizing AI to Tackle Global Ecological Challenges. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 49-57.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p57

[36]. Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 57-69.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p69

[37]. Padmanaban, H. (2024). Navigating the Role of Reference Data in Financial Data Analysis: Addressing Challenges and Seizing Opportunities. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 69-78.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p78

[38]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p89

[39]. PC, H. P., & Sharma, Y. K. (2024). Developing a Cognitive Learning and Intelligent Data Analysis-Based Framework for Early Disease Detection and Prevention in Younger Adults with Fatigue. *Optimized Predictive Models in Health Care Using Machine Learning*, 273.https://books.google.com.bd/books?hl=en&lr=&id=gtXzEAAAQBAJ&oi=fnd&pg=PA273&dq=Developing+a+Cognitive+Learning+and+Intelligent+Data+Analysis-

Based+Framework+for+Early+Disease+Detection+and+Prevention+in+Younger+Adults+with+Fatigue&ots=wKUZk_Q0IG&sig=WDlXjvDmc77Q7lvXW9MxIh9lz-Q&redir_esc=y#v=onepage&q=Developing%20a%20Cognitive%20Learning%20and%20Intelligent%20Data%20Analysis-Based%20Framework%20for%20Early%20Disease%20Detection%20and%20Prevention%20in%20Younger%20Adults%20with%20Fatigue&f=false

[40]. Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics*, *4*(1), 14–32. Retrieved from https://thesciencebrigade.com/jcir/article/view/116

[41]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572317_Critical_study_of_software_models_used_cloud_application_development/links/65ad55d7ee1e1951fbd79df6/Critical-study-of-software-models-used-cloud-application-development.pdf

[42]. Padmanaban, P. H., & Sharma, Y. K. (2019). Implication of Artificial Intelligence in Software Development Life Cycle: A state of the art review. *vol*, *6*, 93-98.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572222_Implication_of_Artificial_Intelligence_in_Software_Development_Life_Cycle_A_state_of_the_art_review/links/65ad54e5bf5b00662e333553/Implication-of-Artificial-Intelligence-in-Software-Development-Life-Cycle-A-state-of-the-art-review.pdf

[43]. Harish Padmanaban, P. C., & Sharma, Y. K. (2024). Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning. *Advances in Aerial Sensing and Imaging*, 267-294. **https://doi.org/10.1002/9781394175512.ch12**

[44]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.https://patents.google.com/patent/US20230385176A1/en

[45]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412.DOI: https://doi.org/10.60087/jklst.vol2.n3.p412

[46]. PC, H. P. Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence.https://shodhganga.inflibnet.ac.in/handle/10603/487443

[47].Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89. DOI: https://doi.org/10.60087/jaigs.v2i1.p89

[48]. Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

DOI: https://doi.org/10.60087/jaigs.v3i1.75

[49]. Latif, M. A., Afshan, N., Mushtaq, Z., Khan, N. A., Irfan, M., Nowakowski, G., ... &Telenyk, S. (2023). Enhanced classification of coffee leaf biotic stress by synergizing feature concatenation and dimensionality reduction. *IEEE Access*.
DOI: https://doi.org/10.1109/ACCESS.2023.3314590

[50]. Irfan, M., Mushtaq, Z., Khan, N. A., Mursal, S. N. F., Rahman, S., Magzoub, M. A., ... & Abbas, G. (2023). A Scalo gram-based CNN ensemble method with density-aware smote oversampling for improving bearing fault diagnosis. *IEEE Access*, *11*, 127783-127799.
DOI: https://doi.org/10.1109/ACCESS.2023.3332243

[51]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*.

DOI: https://doi.org/10.1109/ACCESS.2023.3326367

[52]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE.

DOI: https://doi.org/10.1109/ETECTE59617.2023.10396717

[53]. Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection. https://doi.org/10.32604/cmc.2024.047621

[54]. Ara, A., &Mifa, A. F. (2024). INTEGRATING ARTIFICIAL INTELLIGENCE AND BIG DATA IN MOBILE HEALTH: A SYSTEMATIC REVIEW OF INNOVATIONS AND CHALLENGES IN HEALTHCARE SYSTEMS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(01), 01-16.

DOI: https://doi.org/10.62304/jbedpm.v3i01.70

[55]. Bappy, M. A., & Ahmed, M. (2023). ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH MACHINE LEARNING MODELS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 15-26.
DOI: https://doi.org/10.62304/jbedpm.v2i04.67

[56]. Bappy, M. A. (2024). Exploring the Integration of Informed Machine Learning in Engineering Applications: A Comprehensive Review. *American Journal of Science and Learning for Development*,

3(2), 11-21.
DOI: https://doi.org/10.51699/ajsld.v3i2.3459

[57]. Uddin, M. N., Bappy, M. A., Rab, M. F., Znidi, F., &Morsy, M. (2024). Recent Progress on Synthesis of 3D Graphene, Properties, and Emerging Applications.
DOI: https://doi.org/10.5772/intechopen.114168

[58]. Hossain, M. I., Bappy, M. A., &Sathi, M. A. (2023). WATER QUALITY MODELLING AND ASSESSMENT OF THE BURIGANGA RIVER USING QUAL2K. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(03), 01-11.
DOI: https://doi.org/10.62304/jieet.v2i03.64