World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Graph-based security models for AI-driven data storage: A novel approach to protecting classified documents

Eliel Kundai Zhuwankinyu [1,*], Munashe Naphtali Mupa [2] and Sylvester Tafirenyika [2]

[1] *Illinois Institute of Technology.*
[2] *Hult International Business School.*

World Journal of Advanced Research and Reviews, 2025, 26(02), 1108-1124

Publication history: Received on 25 March 2025; revised on 05 May 2025; accepted on 08 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1631

Abstract

Corporate data storage systems are susceptible to cyber threats; thus, securing them is a central problem in Artificial Intelligence (AI). Graph-Based Security Models (GBSM) form a reliable and scalable approach to reinforcing cybersecurity. These models help to map out extended cyber threats comprehensively and facilitate enhanced threat identification, anomaly detection, and cryptographic integrity. Special emphasis has to do with integrating AI with GBSM as it enhances real-time anomaly detection, automated threat response, cryptographic computing, and other approaches that make it a helpful solution for the secured handling of classified documents in fluid technological contexts.

This work examines the specific problem of how traditional approaches to implementing information security are ineffective against, for example, zero-day exploits and advanced persistent threats. GBSM, therefore, provides more versatile security measures for defence, which are brought about by the constant analysis of relationships between different entities in different threat vectors. Additionally, advanced elements of cryptography key management and decentralized blockchain frameworks add more strength to the protection of identity and valuables, giving the advantage of a nearly unalterable and transparent access control, which are remedies for modern security needs.

The proposed study focuses on integrating GBSM and AI to defend distributed systems and cloud environments. It explains how these models allow organizations to map out and recognize threats and address them before they occur in a decentralized environment. Besides, the application of graph-based methods in quantum-safe cryptography and blockchain applications makes it possible to develop protection against novel threats in quantum computing and adversarial actions.

By using programs that utilize artificial intelligence, this article explores a progressive outlook on the issue of cybersecurity. Here, he saves a place for the comprehensiveness of future security frameworks enriched by AI, quantum cryptography, and GBSM, which should be suitable for future increased threats. Furthermore, the study recommends that future works to solve the outlined issues must develop adaptive AI models that include post-quantum cryptographic methods for protecting data when faced with new technological threats.

Keywords: Artificial Intelligence; Classified; Data; Graph-based; Models

1. Introduction

Graph-Based Security Models (GBSM) is an advanced cybersecurity paradigm that leverages graph-theoretic structures to analyze, detect, and mitigate cyber threats in AI-driven data storage environments. GBSM provides a scalable and

* Corresponding author: Eliel Kundai Zhuwankinyu

adaptable security framework that enhances anomaly detection, cryptographic integrity, and access control mechanisms by representing cybersecurity events as interconnected nodes within a graph structure (Liu et al., 2022). This approach facilitates the identification of complex attack vectors that traditional models struggle to address.

Given the increasing volume and complexity of cyber threats, AI-driven data storage security is critical for protecting classified documents. The integration of AI enhances security operations by enabling real-time detection of anomalies, automating security policy management, and improving incident response times (Adenekan, 2024). When combined with GBSM, AI models provide enhanced security against adversarial attacks by leveraging graph-based anomaly detection and advanced cryptographic techniques (Al Siam et al., 2025).

Traditional security models rely on rule-based and signature-based detection mechanisms, often failing against sophisticated threats such as zero-day exploits and advanced persistent threats (Nagpure, 2024). In contrast, GBSM can dynamically adapt to evolving threat landscapes by continuously analyzing relationships between entities, making them superior in real-time security applications (Casas et al., 2023). As distributed networks and cloud-based infrastructures become more prevalent, the need for adaptive security models is paramount. Graph-based approaches enable organizations to visualize attack surfaces more effectively, allowing for proactive mitigation of threats in decentralized architectures (Ejeofobiri et al., 2024). Additionally, GBSM contributes to cryptographic applications by enhancing key management systems and detecting anomalies in encrypted traffic (Tarafdar, 2024).

This paper explores how GBSM improves security frameworks through AI-enhanced threat detection, cryptographic applications, and real-time adaptive security models. By integrating AI with graph-based structures, GBSM offers a robust, scalable, and proactive approach to securing classified documents in an increasingly complex digital landscape (Ejjami, 2024).

1.1. The Implications of Graph-Based Security Models on Traditional, Blockchain, and AI-Based

1.1.1. Key Security

Graph-based approaches in cryptographic models improve key security by structuring key management through complex relationships and secure mappings. Fuzzy graph theory has been explored to enhance key management efficiency, enabling more secure cryptographic systems (Singh, Khalid, and Nishad, 2024). A knowledge graph-based approach also strengthens security policies by mapping access control methods to secure encrypted communication (Chen et al., 2024). Additionally, blockchain-based cryptographic models integrate graph security to prevent unauthorized decryption (Tsoulias et al., 2020). Tree-based cryptographic access control enhances distributed key management, ensuring security in multi-user environments (Alderman, Farley, and Crampton, 2017). Such approaches provide scalable, attack-resistant cryptographic models.

Moreover, Graph-Based Security Models (GBSMs) enhance blockchain-based key security by providing structured cryptographic methods for decentralized authentication and access control (Wan et al., 2024). The decentralized and immutable nature of blockchain aligns with graph-based security, ensuring transparent and tamper-proof key management (De Alwis, Pham, and Liyanage, 2022). In Industry 4.0, blockchain-integrated GBSMs secure transactions and enforce cryptographic policies (Bhattacharya et al., 2021). These approaches optimize key security while supporting scalable, AI-driven threat detection in emerging technologies (Porambage and Liyanage, 2023).

AI-enhanced cryptographic key management revolutionizes access control by improving security, efficiency, and scalability in AI-driven storage environments. Adaptive AI-driven encryption dynamically adjusts key management strategies, reducing vulnerabilities inherent in static cryptographic models (Ahmad et al., 2025). AI-driven identity and access management (IAM) further strengthens authentication protocols, minimizing unauthorized access risks (Rehman and Ali, 2024). AI-integrated blockchain solutions provide additional security layers, ensuring decentralized and immutable key storage (Ruzbahani, 2024).

Graph security models strengthen zero-trust architectures by mitigating key compromise risks through continuous access validation and anomaly detection (Ahmadi, 2024). These models implement micro-segmentation, preventing lateral movement of threats in case of credential breaches (Ghasemshirazi, Shirvani, and Alipour, 2023). Graph-based analytics dynamically monitor authentication behaviors, improving key security through automated threat responses (Syed et al., 2022). Additionally, these models provide robust cryptographic key distribution, preventing insider threats by validating entities based on real-time risk assessments (Alevizos, Eiza, and Ta, 2022).

Graph-based key security also offers enhanced scalability and resilience compared to traditional Public Key Infrastructure (PKI) by utilizing decentralized trust models (Guru et al., 2023). A case study in financial services demonstrated that graph-based security reduced cryptographic overhead while maintaining high authentication integrity (Kahmann et al., 2023). Unlike PKI, which relies on centralized Certificate Authorities (CAs), graph-based methods offer more robust resistance to quantum-based threats (Salama, Shams, and Bhatnagar, 2023). These models enhance key distribution efficiency and security flexibility in decentralized networks (Maldonado-Ruiz, Torres, and El Madhoun, 2022).

1.2. Implications of Graph-Based Security on Quantum Cryptography and AI in Threat Analysis

Quantum cryptography (QC) leverages quantum mechanics to enhance secure communication, particularly through Quantum Key Distribution (QKD), which ensures unconditional security against computational attacks (Sood, 2024). However, quantum computers pose a significant threat to classical cryptographic systems, as Shor's algorithm enables efficient factorization of large numbers, breaking RSA and ECC encryption (Hosseini and Pilaram, 2024). Post-quantum cryptography (PQC) aims to develop quantum-resistant algorithms, with lattice-based and hash-based cryptography emerging as promising alternatives (Li et al., 2023). The transition to PQC presents challenges, including standardization, performance trade-offs, and infrastructure adaptation (Sharma et al., 2023).

Graph-based security models provide enhanced resilience against quantum attacks by structuring key management and authentication mechanisms with quantum-resistant cryptographic protocols (Oliva delMoral and deMarti iOlius, 2024). These models integrate with post-quantum cryptography by employing hash-based and lattice-based encryption schemes to prevent quantum-based key compromise (Singamaneni and Muhammad, 2024). Additionally, graph structures improve distributed ledger security, ensuring cryptographic operations remain secure in quantum environments (Xu et al., 2023). Their role in securing key exchanges and reinforcing cryptographic trust frameworks makes them crucial for future quantum-safe infrastructure (Thanalakshmi et al., 2021).

AI-driven security enhances distributed network protection by employing real-time anomaly detection and automated threat response mechanisms (Kavitha and Thejas, 2024). Deep learning models analyze network behavior to identify complex threat vectors, enabling proactive security measures (Tan et al., 2024). AI-driven mapping of cyber threats allows for the identification of attack strategies and improves adaptive security policies (Paracha et al., 2024). These solutions reduce response times and mitigate large-scale distributed denial-of-service (DDoS) attacks in decentralized systems (Zacharis, Katos, and Patsakis, 2024).

Graph-theory-based anomaly detection enhances AI-powered Security Operations Centers (SOCs) by mapping cybersecurity threats through graph analytics, reducing dwell time in attack detection (Rahman, 2024). These techniques utilize graph structures to represent complex security events, improving AI-driven threat correlation and predictive analytics (El Azzaoui et al., 2020). Graph-based anomaly detection enhances automated security responses, enabling SOCs to prioritize and mitigate cyber incidents efficiently (Md Shariar Sozol et al., 2024). By integrating AI with graph algorithms, SOCs improve situational awareness, proactively detecting and preventing advanced persistent threats in real-time.

Graph-based threat visualization enhances Cyber Threat Intelligence (CTI) by enabling security analysts to map attack patterns and relationships among cyber threats (Jia et al., 2025). AI-driven CTI platforms utilize graph analytics to extract insights from structured and unstructured data, improving situational awareness (Bratsas, Anastasiadis, and Angelidis, 2024). Advanced persistent threat (APT) detection is significantly improved through graph-based algorithms that analyze threat intelligence reports (Gulbay and Demirci, 2024). These methods automate attack vector correlation, reducing detection time and enabling proactive cybersecurity strategies (Li et al., 2023).

AI-powered real-time threat detection in distributed networks also enhances cybersecurity by identifying anomalies and mitigating attacks before they escalate (Rehman and Weng, 2025). Federated learning models improve distributed threat detection by training AI algorithms without exposing sensitive data (Anandharaj, 2024). AI-driven platforms enable continuous network monitoring and rapid response to threats like Distributed Denial-of-Service (DDoS) attacks (Mirza and Huider, 2024). These solutions significantly enhance cybersecurity resilience by reducing response times and automating security protocols (Abdel-Wahid, 2024).

1.3. Implications for Big Data, IoT Security, and Future Directions

Graph-based security models provide scalable and efficient mechanisms for securing large-scale big data infrastructures by enabling real-time anomaly detection and attack correlation (Win, Tianfield, and Mair, 2017). These models use graph-based event correlation to analyze complex attack patterns, enhancing cybersecurity in virtualized cloud

infrastructures. Additionally, graph theory supports big data analytics in IoT environments by facilitating adaptive security policies for heterogeneous devices (Rathore et al., 2021).

The increasing complexity of IoT networks requires robust security frameworks to mitigate cyber threats. Graph-based techniques efficiently identify IoT vulnerabilities by analyzing abnormal traffic patterns and detecting outliers in network behavior (Gao et al., 2023). Additionally, these models enhance survivability assessments by optimizing intrusion prevention strategies for IoT applications (Shakhov and Koo, 2021). A novel graph-based approach has also been applied to IoT botnet detection, improving resilience against distributed denial-of-service (DDoS) attacks (Nguyen, Ngo, and Le, 2020). These security advancements demonstrate the critical role of graph-based security models in protecting large-scale infrastructures.

Moreover, AI-driven IoT data management presents significant privacy concerns, particularly in securing sensitive data from unauthorized access and misuse (Marengo, 2024). The integration of AI in IoT systems enables real-time data processing but increases exposure to cyber threats and data breaches. Transparent data governance frameworks are necessary to ensure compliance with global privacy regulations such as GDPR and CCPA (Marengo, 2024). Privacy-preserving AI techniques, including differential privacy and homomorphic encryption, are being adopted to mitigate these risks while maintaining efficient IoT data operations (Castro, Deng, and Park, 2023).

Graph AI-driven anomaly detection enhances IoT security by identifying cyber threats and network anomalies through advanced pattern recognition techniques (Salem, Said, and Nour, 2024). These models leverage Graph Neural Networks (GNNs) to detect real-time security threats and automate intrusion detection (Ejeofobiri, Victor-Igun, and Okoye, 2024). AI-enhanced anomaly detection frameworks significantly improve IoT reliability, reducing false positives in cyber threat detection (Wajid and Sans, 2024). These solutions offer scalable, proactive security measures essential for the growing IoT ecosystem.

Autonomous security frameworks for IoT are emerging as a critical research direction to address the increasing complexity of cyber threats. AI-driven adaptive security models are being developed to enhance threat intelligence and automated response mechanisms in 5G-enabled IoT ecosystems (Abie and Pirbhulal, 2024). Decentralized security approaches, such as blockchain-integrated AI frameworks, are improving IoT device authentication and data integrity (Figueiredo et al., 2022). Future advancements will also focus on autonomous intrusion detection using machine learning to mitigate real-time attacks (Akhunzada, Al-Shamayleh, and Zeadally, 2024). These frameworks promise scalable, self-sustaining cybersecurity for next-generation IoT networks.

1.4. Relationship with IoMT (Internet of Medical Things) Secure Data Management Framework

Graph-based security models play a crucial role in protecting Internet of Medical Things (IoMT) devices by providing scalable and adaptive security frameworks. These models use graph analytics to detect and prevent cyber threats by mapping attack vectors and identifying vulnerabilities in real-time (Lofù, 2022). By leveraging graph-based anomaly detection, IoMT networks can proactively mitigate risks associated with unauthorized access and data breaches (Karaarslan and Konacaklı, 2021). AI-enhanced graph security further improves real-time threat intelligence, automating detection mechanisms to safeguard IoMT devices from emerging cyber threats (Wen, Shukla, and Katt, 2025).

AI-powered security graphs enhance healthcare data privacy by ensuring robust encryption, secure access control, and compliance with regulatory standards. Graph neural networks (GNNs) support the implementation of decentralized privacy frameworks, reducing the risk of centralized data breaches (Singh and Siddiqui, 2024). These models allow for efficient anonymization of patient records, enabling privacy-preserving AI applications in electronic health records (EHRs) (Khalid et al., 2023). Furthermore, AI-driven privacy-preserving techniques, such as federated learning, ensure secure medical data processing without compromising patient confidentiality (Majeed, Khan, and Hwang, 2022). These advancements highlight the transformative impact of AI-powered security graphs in safeguarding sensitive healthcare information.

Graph-based threat intelligence enhances attack vector analysis in Internet of Medical Things (IoMT) environments by mapping cyber threats and identifying vulnerabilities in healthcare networks (Naghib, Gharehchopogh, and Zamanifar, 2025). These models detect and visualize attack paths in IoMT systems, mitigating risks posed by weak authentication, unencrypted data transmission, and outdated security protocols (Ghodsizad, 2024). Graph-based security models effectively counter man-in-the-middle (MITM) and Sybil attacks in IoMT by leveraging machine learning for adaptive anomaly detection (Nagamani and Kumar, 2024). Furthermore, graphical security modeling (GSM) has been implemented to assess and prevent attack propagation across interconnected IoMT devices (AboulEla et al., 2024).

A case study on hospital network security highlights the effectiveness of graph-based security models in preventing cyber threats in healthcare cloud storage (Ravi, Pham, and Alazab, 2022). AI-driven security graphs strengthen healthcare data transmission security by proactively identifying suspicious activity and optimizing access control policies (Naphtali Mupa et al., 2025). Cloud-based IoMT frameworks integrate graph analytics to protect patient records and encrypted medical data from ransomware and unauthorized access (Prasad et al., 2022). This research underscores the necessity of graph-based security in modern healthcare infrastructures.

Graph-based security frameworks also enhance regulatory compliance by automating data protection and ensuring adherence to privacy laws such as HIPAA and GDPR (Karalka and Meditskos, 2024). These models use graph-based risk management to detect vulnerabilities in data processing and enforce real-time security policies (Aljarrah, Cherbal, and Mashaleh, 2024). Graph property analysis has been applied to privacy threat modeling, improving compliance automation in cloud-based healthcare applications (Kunz, Weiss, and Schneider, 2023). Additionally, knowledge graphs enable structured data access control, enhancing auditability and reducing compliance violations (Sangeetha, Selvarathi, and Mathivanan, 2024). These advancements ensure that organizations efficiently maintain regulatory security and privacy standards.

1.5. The Impact of AI-Driven Enhancements in Cloud Computing Security

AI-powered graph security enhances cloud computing environments by enabling real-time anomaly detection and adaptive threat response mechanisms (Moorthy and Jagannath, 2024). Graph-based models improve cybersecurity in cloud networks by analyzing connections between digital assets, helping detect and neutralize cyber threats efficiently (Ullah, Kamal, and Asif, 2024). Additionally, AI-driven security graphs support automated compliance monitoring, reducing human intervention while ensuring regulatory adherence (Ankalaki et al., 2025).

The synergy between ML, Generative AI, and graph-based cybersecurity is transforming threat intelligence. Machine learning models use graph-based analytics to uncover complex attack patterns, strengthening intrusion detection systems (IDS) (Zhang et al., 2024). Generative AI further enhances cybersecurity by predicting potential attack vectors and optimizing security responses (Al Siam et al., 2025). These AI-driven technologies, when integrated with graph-based security frameworks, enable scalable and self-learning security infrastructures capable of proactive cyber defense (Sindiramutty and Prabagaran, 2025).

Zero-trust architecture (ZTA) is revolutionizing AI-driven cloud security by eliminating implicit trust and enforcing strict access controls based on continuous verification (Ahmadi, 2025). Unlike perimeter-based models, ZTA integrates AI-driven authentication and graph-based policy enforcement to mitigate unauthorized access risks (Xun et al., 2025). AI-driven ZTA enhances real-time threat detection by leveraging graph analytics to analyze attack patterns and predict intrusion attempts (Jern et al., 2025). Moreover, integrating adaptive multi-factor authentication (MFA) within ZTA models ensures improved security resilience against sophisticated cyber threats (Nagpure, 2024).

Supply chain attacks in multi-cloud environments are becoming more prevalent, necessitating AI-driven graph-based security approaches (Joshi, 2024). Graph-based threat intelligence maps vulnerabilities across interconnected cloud providers, identifying potential breach points before exploitation (Hassan, Nizam-Uddin, and Quddus, 2024). AI-driven topology graph-based anomaly detection (TOGBAD) models further enhance supply chain security by identifying anomalies in data flows and transaction logs (Ge, 2024). This integration of AI, ZTA, and graph-based security ensures a resilient defense against evolving cyber threats in multi-cloud infrastructures.

AI-enhanced graph-based security is transforming cloud security in AWS, Azure, and Google Cloud by improving risk mitigation and real-time anomaly detection (Xun et al., 2025). AWS utilizes topology graph-based anomaly detection (TOGBAD) to identify security threats within its infrastructure, strengthening access control mechanisms (Hassan, Nizam-Uddin, and Quddus, 2024). Similarly, Azure integrates AI-driven schedulers and graph-based lineage inference models to enhance security visibility and ensure cloud workload protection (Naphtali Mupa et al., 2025). Google Cloud leverages distributed tracing and graph-based detection methods to monitor cloud service interactions and automate security responses (Rallabandi, 2024). These advancements in AI-powered cloud security underscore the growing reliance on graph-based threat intelligence.

2. AI-Powered Threat Hunting in SAP and ERP Environments

AI-driven cybersecurity enhances enterprise environments by improving threat detection, fraud prevention, and security automation (Moore and Routhu, 2024). Enterprises are leveraging AI-powered security solutions to enhance

risk assessment, integrating machine learning algorithms with cybersecurity protocols to identify potential security breaches in real time (Luntovskyy et al., 2024).

Graph-based anomaly detection plays a vital role in securing SAP and ERP systems by mapping network behavior, identifying abnormal patterns, and mitigating data breaches (Stufano, 2024). By integrating graph-based machine learning, ERP security frameworks can detect fraudulent activities within enterprise resource planning environments (Eliel et al., 2025). This ensures organizations maintain robust cybersecurity postures and comply with regulatory requirements.

Insider threats and Advanced Persistent Threats (APTs) present major security risks in Enterprise Resource Planning (ERP) frameworks, often bypassing traditional security controls to exploit privileged access (Rodrigues, 2019). AI-driven security models use behavioral analytics to detect anomalous user activities, preventing unauthorized access to critical ERP data. Graph-based anomaly detection plays a crucial role in identifying fraudulent transactions, safeguarding financial and operational data from manipulation (Tan et al., 2025).

A case study on SAP security reveals that graph-based threat intelligence effectively detects privilege escalation by mapping access control relationships and monitoring deviations from normal usage patterns (Rodrigues, 2019). By analyzing role inheritance and access hierarchies, organizations can proactively mitigate unauthorized privilege escalation attempts in ERP systems. This graph-based security approach enhances the visibility of attack paths, allowing for rapid response to emerging threats (Mehmood et al., 2023).

2.1. Security Threats in AI-Driven Cloud Environments

AI-driven cloud environments face a growing number of security threats, including adversarial attacks, data poisoning, and model inversion. Adversarial attacks manipulate input data to deceive AI models, leading to incorrect predictions and potential system compromise (Zhuwankinyu et al., 2023). Data poisoning introduces corrupted training data to alter AI model behavior, reducing accuracy and increasing vulnerabilities (Reddy, Konkimalla, & Rajaram, 2022). Model inversion attacks extract sensitive data from trained models, raising privacy concerns (Alaca, Celık, & Goel, 2023).

Containerized AI environments, particularly those using Kubernetes, present security risks such as container escapes, where malicious actors gain access to the host system, and Kubernetes cluster attacks, targeting misconfigurations and privilege escalation (Mitropoulou, Kokkinos, & Soumplis, 2024). Cloud-based AI security is further threatened by unauthorized access, API abuse, and data leakage, particularly in multi-cloud deployments (Wijenayake & Henna, 2023).

Graph-Based Security Models (GBSM) provide a structural approach to identifying vulnerabilities in AI-driven workflows by mapping attack surfaces and tracking malicious activities (Grata, Deshpande, & Lopes, 2024). Graph analytics enhances predictive threat detection, improving AI model resilience in multi-cloud and containerized AI deployments (Nagpure, 2024).

GBSM facilitates attack path visualization in complex AI workflows, allowing for proactive security measures in cloud infrastructures (Khan, Matskin, & Prodan, 2024). By integrating knowledge graphs and machine learning, security models detect anomalies in AI model interactions and prevent potential adversarial threats (Zhong et al., 2024). These solutions significantly enhance AI security by monitoring containerized applications, enforcing zero-trust authentication, and preventing model manipulation attacks (Nguyen, Zhu, & Liu, 2022).

2.2. Incorporating Advanced Security Techniques in Graph-Based Models

Differential privacy (DP) is a technique that ensures AI models do not expose individual data points, maintaining strong privacy guarantees (Luo et al., 2024). It is widely used in cloud-based AI platforms, such as Google AI, Microsoft Azure ML, and AWS Sagemaker, to prevent re-identification attacks during model training (Qiu et al., 2022). Graph-Based Security Models (GBSM) track data anonymization by applying differential privacy techniques to encrypted graph nodes, ensuring robust privacy-preserving AI operations (Fu et al., 2023).

Federated learning (FL) enables decentralized model training across multiple devices without sharing raw data, mitigating privacy risks (Mansour Bahar, Ferrahi & Messai, 2024). However, FL remains vulnerable to security threats such as model inversion and poisoning attacks, where adversaries manipulate training updates to infer sensitive data (Han et al., 2024). GBSM enhances FL security by identifying anomalous patterns in model updates, flagging potentially compromised nodes in decentralized AI workflows (Luo et al., 2023). In practice, FL combined with graph-based anomaly detection is applied in cloud environments like GCP Vertex AI and Azure AI to secure collaborative AI training (Pauu et al., 2023).

Encryption plays a critical role in AI security, with homomorphic encryption allowing computations on encrypted data, preserving privacy (Zhang, 2023). End-to-end encryption ensures secure communication in AI workflows by preventing unauthorized access (Ye et al., 2023). GBSM improves encryption-based security policies by mapping cryptographic trust structures, enhancing compliance in cloud-based AI models (Fu et al., 2023). In Google Cloud Platform (GCP), confidential computing utilizes graph-based security to reinforce AI model protection, ensuring data confidentiality in training and deployment (K Zhang, 2023).

Data masking plays a crucial role in securing sensitive AI training datasets by obfuscating personally identifiable information (PII) while maintaining analytical integrity (Chen et al., 2024). Graph-Based Security Models (GBSM) enhance this by tracking masked data flows to prevent unauthorized exposure in AI workflows (Jia et al., 2024). In cloud AI applications, data masking is vital in healthcare and financial services to protect sensitive records while enabling predictive analytics (Nandan, Mitra & De, 2025).

Zero Trust Architecture (ZTA) also ensures AI security through continuous verification and least-privilege access, eliminating implicit trust in cloud environments (Xin et al., 2025). Graph-based authentication strengthens ZTA by monitoring access pathways and preventing unauthorized lateral movement (Gambo & Almulhem, 2025). Google's BeyondCorp implements ZTA principles for AI security, integrating graph-based access control to protect AI-driven cloud services (Ye et al., 2024).

2.3. Practical Implementation: Securing AI Containers and Workflows with Graph-Based Security

AI containerized environments, such as Kubernetes, are susceptible to vulnerabilities including supply chain attacks and privilege escalation (Athukorale et al., 2025). Graph-Based Security Models (GBSM) can mitigate these threats by employing attack graph visualization to detect malicious activity in AI clusters (Mitra et al., 2024). In cloud-based Kubernetes deployments, integrating GBSM enhances security through anomaly detection and predictive threat monitoring (Nguyen, Zhu & Liu, 2022).

Google Cloud's Anthos and AI Platform leverage graph-based security models to strengthen AI pipeline security (Patel et al., 2024). GBSM is particularly useful for graph-enhanced intrusion detection, which safeguards AI workflows from data exfiltration and adversarial model manipulations (Rallabandi, 2024). By integrating graph analytics with Google Cloud Functions, these models enhance AI execution while maintaining container-based isolation (Wijenayake & Henna, 2023).

In terms of future trends, quantum-safe cryptography is an emerging trend in AI-driven cloud security, addressing the risks posed by quantum computing to traditional encryption methods (Grata, Deshpande & Lopes, 2024). However, implementing graph-based security at scale is challenging due to the complexity of handling large-scale graph computations and real-time threat detection (Zhong et al., 2024). The need for AI-driven security automation in graph-based threat intelligence is growing, as manual threat response is inefficient in dynamic cloud environments (Ramya, Smera & Sandeep, 2025). AI-based anomaly detection enhances predictive cybersecurity by identifying risks before exploitation occurs (Adenekan, 2024).

3. Recommendation and Conclusion

This article explored the significance of Graph-Based Security Models (GBSMs) in AI-driven data storage, highlighting their role in mitigating cyber threats, preventing key compromises, and enhancing cryptographic applications (Paul, 2024). We examined AI-enhanced cryptographic key management, graph-based anomaly detection, and the integration of quantum-safe cryptography to secure sensitive data in enterprise and cloud environments. The study further analyzed case studies on AWS, Azure, and Google Cloud, demonstrating how graph security enhances multi-cloud resilience, IoT, and ERP security (Rachid Ejjami, 2024).

To address evolving cyber threats, organizations should integrate Artificial Intelligence (AI), Quantum Cryptography, and Graph-Based Security into cybersecurity frameworks (Dhanamma Jagli, 2024). AI-driven graph analytics should be leveraged for real-time attack detection, insider threat mitigation, and supply chain security (Kelvin Ovabor et al., 2024). Future research should focus on adaptive AI models that integrate post-quantum cryptographic techniques, ensuring security against emerging quantum computing threats.

Further advancements in graph-based cybersecurity frameworks should emphasize autonomous security decision-making, reducing manual intervention. Federated learning models, zero-trust architectures, and blockchain-enhanced access control should be integrated with graph-driven risk assessment to secure decentralized infrastructures (Freed

& Jackson, 2022). Additionally, real-time policy enforcement using AI-based regulatory compliance monitoring will strengthen security governance (Joshi, 2025).

From a policy perspective, governments and industry leaders must establish standardized ethical AI security guidelines to ensure responsible implementation. Regulatory bodies such as HIPAA, GDPR, and NIST should refine frameworks to address AI-driven cybersecurity risks in critical sectors (Lund et al., 2025). Ethical AI security measures must prioritize transparency, fairness, and bias mitigation, ensuring robust and trustworthy cybersecurity ecosystems. Graph-based security models will continue to shape the future of AI-driven cybersecurity, offering scalable, intelligent, and adaptive security solutions for complex cyber threats (NIST, 2021).

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdel-Wahid, T. (2024) 'AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention', ResearchGate. Available at: https://www.researchgate.net/profile/Research-Scholar-Ii/publication/383095008_AI-POWERED_CLOUD_SECURITY_A_STUDY_ON_THE_INTEGRATION_OF_ARTIFICIAL_INTELLIGENCE_AND_MACHINE_LEARNING_FOR_IMPROVED_THREAT_DETECTION_AND_PREVENTION/links/66bc8afe145f4d355357f81b/AI-POWERED-CLOUD-SECURITY-A-STUDY-ON-THE-INTEGRATION-OF-ARTIFICIAL-INTELLIGENCE-AND-MACHINE-LEARNING-FOR-IMPROVED-THREAT-DETECTION-AND-PREVENTION.pdf (Accessed: 12 March 2025).

[2] Abie, H. and Pirbhulal, S. (2024) 'Autonomous Adaptive Security Framework for 5G-Enabled IoT', arXiv. DOI: 10.48550/arXiv.2406.03186 (Accessed: 12 March 2025).

[3] AboulEla, S., Ibrahim, N., Shehmir, S., Yadav, A., and Kashef, R. (2024) 'Navigating the cyber threat landscape: An in-depth analysis of attack detection within IoT ecosystems', MDPI AI. DOI: 10.3390/ai5020037 (Accessed: 12 March 2025).

[4] Adenekan, T.K. (2024) 'Optimized AI and Graph-Regularized Neural Networks for Cyber Security and AIOps in IoT', ResearchGate. Available at: https://www.researchgate.net/profile/Tobiloba-Adenekan/publication/386441217_Optimized_AI_and_Graph-Regularized_Neural_Networks_for_Cyber_Security_and_AIOps_in_IoT/links/675176d1e17ef87d1de64998/Optimized-AI-and-Graph-Regularized-Neural-Networks-for-Cyber-Security-and-AIOps-in-IoT.pdf [Accessed 14 March 2025].

[5] Adenekan, T.K. (2024) Optimized AI and Graph-Regularized Neural Networks for Cyber Security and AIOps in IoT. ResearchGate. Available at: https://www.researchgate.net/profile/Tobiloba-Adenekan/publication/386441217_Optimized_AI_and_Graph-Regularized_Neural_Networks_for_Cyber_Security_and_AIOps_in_IoT/links/675176d1e17ef87d1de64998/Optimized-AI-and-Graph-Regularized-Neural-Networks-for-Cyber-Security-and-AIOps-in-IoT.pdf (Accessed: 12 March 2025).

[6] Ahmad, A., Rehman, A.U., Ghani, M.U., Nasim, F., and Naseem, S. (2025) 'An In-Depth Comparative Analysis of Traditional vs AI-Enhanced Encryption Algorithms', Al-Aasar Journal. Available at: http://al-aasar.com/index.php/Journal/article/view/147 (Accessed: 12 March 2025).

[7] Ahmadi, S. (2024) Zero trust architecture in cloud networks: Application, challenges and future opportunities. HAL Science. Available at: https://hal.science/hal-04456272/ (Accessed: 12 March 2025).

[8] Ahmadi, S. (2025) 'Autonomous Identity-Based Threat Segmentation in Zero Trust Architectures', arXiv. DOI: 10.48550/arXiv.2501.06281 (Accessed: 12 March 2025).

[9] Akhunzada, A., Al-Shamayleh, A.S., and Zeadally, S. (2024) 'Design and performance of an AI-enabled threat intelligence framework for IoT-enabled autonomous vehicles', ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S0045790624005366 (Accessed: 12 March 2025).

[10] Al Siam, A., Alazab, M., Awajan, A. and Faruqui, N. (2025) 'A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10836696/ (Accessed: 12 March 2025).

[11] Alaca, Y., Celık, Y. and Goel, S. (2023) 'Anomaly detection in cyber security with graph-based LSTM in log analysis', Chaos Journal. Available at: https://dergipark.org.tr/en/pub/chaos/article/1348302 [Accessed 14 March 2025].

[12] Alderman, J., Farley, N. and Crampton, J. (2017) 'Tree-based cryptographic access control', in Lecture Notes in Computer Science. Springer. Available at: https://link.springer.com/chapter/10.1007/978-3-319-66402-6_5 (Accessed: 12 March 2025).

[13] Alevizos, L., Eiza, M.H., and Ta, V.T. (2022) 'Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9862967/ (Accessed: 12 March 2025).

[14] Aljarrah, S.J., Cherbal, S., and Mashaleh, A. (2024) 'On the Comparative Analysis of Trends in Cybersecurity Risk Assessment, Governance, and Compliance Frameworks', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10847280/ (Accessed: 12 March 2025).

[15] Anandharaj, N. (2024) 'AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention', ResearchGate. Available at: https://www.researchgate.net/profile/Journal-Pub/publication/382527337_AI-Powered_Cloud_Security_A_Study_on_the_Integration_of_Artificial_Intelligence_and_Machine_Learning_for_Improved_Threat_Detection_and_Prevention/links/66a1c36127b00e0ca43e65d1/AI-Powered-Cloud-Security-A-Study-on-the-Integration-of-Artificial-Intelligence-and-Machine-Learning-for-Improved-Threat-Detection-and-Prevention.pdf (Accessed: 12 March 2025).

[16] Ankalaki, S., Rajesh, A.A., Pallavi, M., and Hukkeri, G.S. (2025) 'Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10909100/ (Accessed: 12 March 2025).

[17] Athukorale, N.K., Yi, C.J., Loh Zi Xin, A.Y., Qi, C.J. and Yu, D.Z. (2025) 'Evaluating Advanced Cybersecurity Technologies for Cloud Environments', Preprints. Available at: https://www.preprints.org/frontend/manuscript/c7af352449b61cc7392930a6887c269c/download_pub [Accessed 14 March 2025].

[18] Bhattacharya, P., Saraswat, D., Dave, A., and Acharya, M. (2021) 'Coalition of 6G and blockchain in AR/VR space: Challenges and future directions', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9656726/ (Accessed: 12 March 2025).

[19] Bratsas, C., Anastasiadis, E.K., and Angelidis, A.K. (2024) 'Knowledge Graphs and Semantic Web Tools in Cyber Threat Intelligence: A Systematic Literature Review', Journal of Cybersecurity and Privacy, 4(3), Article 25. DOI: 10.3390/jcp4030025 (Accessed: 12 March 2025).

[20] Casas, P., Vanerio, J., Ullrich, J. and Findrik, M. (2023) GRAPHSEC: Advancing the Application of AI/ML to Network Security Through Graph Neural Networks. Springer. Available at: https://books.google.com/books?hl=en&lr=&id=5CnKEAAAQBAJ&oi=fnd&pg=PA56&dq=graph-based+security+models+for+ai-driven+data+storage+and+cybersecurity&ots=Soi3RKBMQS&sig=yauZm0sZ628u23ZXtqbv_xjMCnk (Accessed: 12 March 2025).

[21] Castro, O.E.L., Deng, X., and Park, J.H. (2023) 'Comprehensive survey on AI-based technologies for enhancing IoT privacy and security: Trends, challenges, and solutions', HCISJ. Available at: http://hcisj.com/data/file/article/2023080005/13-39.pdf (Accessed: 12 March 2025).

[22] Chen, C., Zhang, X., Qiu, H., Lou, J., Liu, Z. and Chen, X. (2024) 'MaskArmor: Confidence masking-based defense mechanism for GNN against MIA', Information Sciences. Available at: https://www.sciencedirect.com/science/article/pii/S0020025524004924 [Accessed 14 March 2025].

[23] Chen, Y., Hu, T., Lou, F., Yin, M., Zeng, T., Wu, G. and Wang, H. (2024) 'A Knowledge Graph-Based Consistency Detection Method for Network Security Policies', Applied Sciences, 14(18), Article 8415. DOI: 10.3390/app14188415 (Accessed: 12 March 2025).

[24] De Alwis, C., Pham, Q.V., and Liyanage, M. (2022) 6G Frontiers: Towards Future Wireless Systems. Available at: https://books.google.com/books?hl=en&lr=&id=7LKeEAAAQBAJ&oi=fnd&pg=PR15&dq=gbsm+integration+with+blockchain-

based+key+security+for+immutable+records&ots=aGbYfsQD7x&sig=aRPaiidFMq_yeh6h8TNBbU2RnXQ (Accessed: 12 March 2025).

[25] Dhanamma Jagli. (2024). The Role of Artificial Intelligence in Cyber Security. Journal of Electrical Systems, 20(3), 5283–5291. https://doi.org/10.52783/jes.6327

[26] Ejeofobiri, C.K., Victor-Igun, O.O. and Okoye, C. (2024) AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks. HAL Science. Available at: https://hal.science/hal-04826235/ (Accessed: 12 March 2025).

[27] Ejjami, R. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. Journal of Next-Generation Research 5.0. https://doi.org/10.70792/jngr5.0.v1i1.5

[28] El Azzaoui, A., Singh, S.K., Pan, Y., and Park, J.H. (2020) 'Block5GIntell: Blockchain for AI-enabled 5G networks', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9159573/ (Accessed: 12 March 2025).

[29] Eliel, K., Zhuwankinyu1, T., Mavenge Moyo, & Mupa, M. (2025). Leveraging Generative AI for an Ethical and Adaptive Cybersecurity Framework in Enterprise Environments. https://www.irejournals.com/formatedpaper/1706753.pdf

[30] Figueiredo, S., Silva, P., Iacovazzi, A., and Holubenko, V. (2022) 'ARCADIAN-IoT: Enabling autonomous trust, security and privacy management for IoT', SpringerLink. Available at: https://link.springer.com/chapter/10.1007/978-3-031-20936-9_28 (Accessed: 12 March 2025).

[31] Freed, G., & Jackson, M. (2022). Zero Trust Architecture in AI-Driven Cybersecurity: A Machine Learning Perspective. ResearchGate. https://doi.org/10.13140/RG.2.2.13125.36320

[32] Fu, D., Bao, W., Maciejewski, R., Tong, H. and He, J. (2023) 'Privacy-preserving graph machine learning from data to computation: A survey', ACM Computing Surveys. DOI: 10.1145/3606274.3606280 [Accessed 14 March 2025].

[33] Gambo, M.L. and Almulhem, A. (2025) 'Zero Trust Architecture: A Systematic Literature Review', TechRxiv. Available at: https://www.techrxiv.org/doi/full/10.36227/techrxiv.173933211.18231232 [Accessed 14 March 2025].

[34] Gao, M., Wu, L., Li, Q., and Chen, W. (2023) 'Anomaly traffic detection in IoT security using graph neural networks', ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S2214212623001163 (Accessed: 12 March 2025).

[35] Garg, N., Wazid, M., Singh, J., and Singh, D.P. (2022) 'Security in IoMT-driven smart healthcare: A comprehensive review and open challenges', Wiley Online Library. DOI: 10.1002/spy2.235 (Accessed: 12 March 2025).

[36] Ge, Y. (2024) 'The Symbiosis of Trust and AI: Scientific Foundations for Strategic Network Security, Autonomous Resilience, and Prescriptive Governance', ProQuest. Available at: https://search.proquest.com/openview/7ff78946fb5901d4f6064a861fd598ff/1?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 12 March 2025).

[37] Ghasemshirazi, S., Shirvani, G., and Alipour, M.A. (2023) 'Zero trust: Applications, challenges, and opportunities', arXiv. DOI: 10.48550/arXiv.2309.03582 (Accessed: 12 March 2025).

[38] Ghodsizad, T. (2024) 'Internet of Medical Things with Considering of Artificial Intelligence', IJSASE. Available at: https://bgsiran.ir/journal/ojs-3.1.1-4/index.php/IJSASE/article/download/121/102 (Accessed: 12 March 2025).

[39] Grata, E.G.H., Deshpande, A. and Lopes, R.T. (2024) 'Artificial intelligence for threat anomaly detection using graph databases–a semantic outlook', Wiley Online Library. DOI: 10.1002/9781394196470.ch13 [Accessed 14 March 2025].

[40] Grata, E.G.H., Deshpande, A. and Lopes, R.T. (2024) 'Artificial intelligence for threat anomaly detection using graph databases–a semantic outlook', Wiley Online Library. DOI: 10.1002/9781394196470.ch13 [Accessed 14 March 2025].

[41] Gulbay, B. and Demirci, M. (2024) 'A Framework for Developing Strategic Cyber Threat Intelligence from Advanced Persistent Threat Analysis Reports Using Graph-Based Algorithms', Preprints.org. Available at: https://www.preprints.org/frontend/manuscript/e75e4611a48eaff7d4dda81a3b1b59be/download_pub (Accessed: 12 March 2025).

[42] Guru, A., Mohanta, B.K., Mohapatra, H., and Al-Turjman, F. (2023) 'A survey on consensus protocols and attacks on blockchain technology', Applied Sciences, 13(4), Article 2604. DOI: 10.3390/app13042604 (Accessed: 12 March 2025).

[43] Han, Z., Hu, C., Li, T., Qi, Q., Tang, P. and Guo, S. (2024) 'Subgraph-level federated graph neural network for privacy-preserving recommendation with meta-learning', Neural Networks, ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S0893608024004982 [Accessed 14 March 2025].

[44] Hassan, A., Nizam-Uddin, N., and Quddus, A. (2024) 'Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity', ResearchGate. Available at: https://www.researchgate.net/profile/Ateeq-Rehman-20/publication/386210978_Navigating_IoT_Security_Insights_into_Architecture_Key_Security_Features_Attacks_Current_Challenges_and_AI-Driven_Solutions_Shaping_the_Future_of_Connectivity/links/674890a4876bd177782b543a/Navigating-IoT-Security-Insights-into-Architecture-Key-Security-Features-Attacks-Current-Challenges-and-AI-Driven-Solutions-Shaping-the-Future-of-Connectivity.pdf (Accessed: 12 March 2025).

[45] Hassan, N.A.B. (2025) 'Managing Data Dependencies in Cloud-Based Big Data Pipelines: Challenges, Solutions, and Performance Optimization Strategies', Orient Academies Journal. Available at: https://orientacademies.com/index.php/OJEPAIAS/article/view/2025-02-10 (Accessed: 12 March 2025).

[46] Hosseini, S.M. and Pilaram, H. (2024) 'A Comprehensive Review of Post-Quantum Cryptography: Challenges and Advances', IACR ePrint Archive. Available at: https://eprint.iacr.org/2024/1940 (Accessed: 12 March 2025).

[47] Jern, C.J., Yan, C.W., Khuan, H.H., Enze, H., and Wee, J.T.K. (2025) 'Cloud Security: Counteracting Evolving Threats in a Digital Age', Preprints.org. Available at: https://www.preprints.org/frontend/manuscript/1d675350f165dcace947b0e032644b90/download_pub (Accessed: 12 March 2025).

[48] Jia, J., Yang, L., Wang, Y., and Sang, A. (2025) 'Hyper attack graph: Constructing a hypergraph for cyber threat intelligence analysis', ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S0167404824004991 (Accessed: 12 March 2025).

[49] Jia, Z., Xiong, Y., Nan, Y., Zhang, Y. and Zhao, J. (2024) '{MAGIC}: Detecting advanced persistent threats via masked graph representation learning', USENIX Security Symposium. Available at: https://www.usenix.org/conference/usenixsecurity24/presentation/jia-zian [Accessed 14 March 2025].

[50] Joshi, H. (2024) 'Emerging Technologies Driving Zero Trust Maturity Across Industries', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10764723/ (Accessed: 12 March 2025).

[51] Joshi, H. (2025). Emerging Technologies Driving Zero Trust Maturity Across Industries. IEEE Open Journal of the Computer Society, 6, 25–36. https://doi.org/10.1109/ojcs.2024.3505056

[52] Kahmann, F., Honecker, F., Dreyer, J., Fischer, M., and Tönjes, R. (2023) 'Performance comparison of directed acyclic graph-based distributed ledgers and blockchain platforms', Computers, 12(12), Article 257. DOI: 10.3390/computers12120257 (Accessed: 12 March 2025).

[53] Karaarslan, E. and Konacaklı, E. (2021) 'Decentralized solutions for data collection and privacy in healthcare', De Gruyter. DOI: 10.1515/9783110668322-008 (Accessed: 12 March 2025).

[54] Karalka, C. and Meditskos, G. (2024) 'Towards a Generic Knowledge Graph Construction Framework for Privacy Awareness', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10679399/ (Accessed: 12 March 2025).

[55] Kavitha, D. and Thejas, S. (2024) 'AI-enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10747338/ (Accessed: 12 March 2025).

[56] Kelvin Ovabor, Ismail Oluwatobiloba Sule-Odu, Travis Atkison, Adetutu Temitope Fabusoro, & Joseph Oluwaseun Benedict. (2024). AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. Open Access Research Journal of Science and Technology, 12(2), 040–048. https://doi.org/10.53022/oarjst.2024.12.2.0135

[57] Khalid, N., Qayyum, A., Bilal, M., and Al-Fuqaha, A. (2023) 'Privacy-preserving artificial intelligence in healthcare: Techniques and applications', ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S001048252300313X (Accessed: 12 March 2025).

[58] Khan, A.Q., Matskin, M. and Prodan, R. (2024) 'Cost modelling and optimization for cloud: a graph-based approach', Journal of Cloud Computing, Springer. Available at: https://link.springer.com/article/10.1186/s13677-024-00709-6 [Accessed 14 March 2025].

[59] Kunz, I., Weiss, K., and Schneider, A. (2023) 'Privacy Property Graph: Towards Automated Privacy Threat Modeling via Static Graph-Based Analysis', Proceedings on Privacy Enhancing Technologies. DOI: 10.56553/popets-2023-0046 (Accessed: 12 March 2025).

[60] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., and Liang, W. (2023) 'Post-quantum security: Opportunities and challenges', Sensors, 23(21), Article 8744. DOI: 10.3390/s23218744 (Accessed: 12 March 2025).

[61] Li, Z.X., Li, Y.J., Liu, Y.W., Liu, C., and Zhou, N.X. (2023) 'K-CTIAA: Automatic Analysis of Cyber Threat Intelligence Based on a Knowledge Graph', Symmetry, 15(2), Article 337. DOI: 10.3390/sym15020337 (Accessed: 12 March 2025).

[62] Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z. and Zhou, Y. (2022) 'Recent progress of using knowledge graph for cybersecurity', Electronics, 11(15), Article 2287. DOI: 10.3390/electronics11152287 (Accessed: 12 March 2025).

[63] Lofù, D. (2022) 'Approaches to Clinical Pathway Protection by means of Artificial Intelligence and Process Mining', Tesi Dottorato. Available at: https://tesidottorato.depositolegale.it/handle/20.500.14242/64143 (Accessed: 12 March 2025).

[64] Lund, B., Orhan, Z., Mannuru, N. R., Bevara, R. V. K., Porter, B., Vinaih, M. K., & Bhaskara, P. (2025). Standards, frameworks, and legislation for artificial intelligence (AI) transparency. AI and Ethics. https://doi.org/10.1007/s43681-025-00661-4

[65] Luntovskyy, A., Klymash, M., Melnyk, I., Beshley, M., and Schill, A. (2024) 'Digital Ecosystems: Interconnecting Advanced Networks with AI Applications', Google Books. Available at: https://books.google.com/books?hl=en&lr=&id=hMcWEQAAQBAJ&oi=fnd&pg=PR5&dq=ai-driven+cybersecurity+in+enterprise+environments+and+graph-based+anomaly+detection+in+sap+and+erp+systems&ots=8C2LoBA9ff&sig=J-bZ0ZFhXL8GAXkrKtli_Rzpais (Accessed: 12 March 2025).

[66] Luo, G., Fang, Z.J., Zhao, X. and Chen, M. (2023) 'A survey of graph federation learning for data privacy security scenarios', Research Square. Available at: https://www.researchsquare.com/article/rs-3183619/latest [Accessed 14 March 2025].

[67] Luo, L., Ren, W., Huang, H. and Wang, F. (2024) 'A Survey on Privacy Attacks and Defenses in Graph Neural Networks', Information Technology and Control, 53(4), pp. 37737. DOI: 10.5755/j01.itc.53.4.37737 [Accessed 14 March 2025].

[68] Majeed, A., Khan, S., and Hwang, S.O. (2022) 'Toward privacy preservation using clustering-based anonymization: recent advances and future research outlook', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9775092/ (Accessed: 12 March 2025).

[69] Maldonado-Ruiz, D., Torres, J., and El Madhoun, N. (2022) 'Current trends in blockchain implementations on the paradigm of public key infrastructure: A survey', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9687536/ (Accessed: 12 March 2025).

[70] Mansour Bahar, A.A., Ferrahi, K.S. and Messai, M.L. (2024) 'FedHE-Graph: Federated Learning with Hybrid Encryption on Graph Neural Networks for Advanced Persistent Threat Detection', ACM International Conference on AI Security and Privacy. DOI: 10.1145/3664476.3670466 [Accessed 14 March 2025].

[71] Marengo, A. (2024) 'Future of AI-Driven IoT: Identifying Emerging Trends in Intelligent Data Analysis and Privacy Protection', Preprints.org. Available at: https://www.preprints.org/manuscript/202312.2184/download/final_file (Accessed: 12 March 2025).

[72] Marengo, A. (2024) 'Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms', ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S2542660524002592 (Accessed: 12 March 2025).

[73] Md Shariar Sozol, Saki, G. M., & Rahman, M. M. (2024). Anomaly Detection in Cybersecurity with Graph-Based Approaches. INTERANTIONAL JOURNAL of SCIENTIFIC RESEARCH in ENGINEERING and MANAGEMENT, 08(008), 1–5. https://doi.org/10.55041/ijsrem37061

[74] Mehmood, M., Amin, R., Muslam, A., Xie, J., & Hamza Aldabbas. (2023). Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. IEEE Access, 11, 46561–46576. https://doi.org/10.1109/access.2023.3273895

[75] Mirza, D. and Huider, F. (2024) 'AI-Powered Information Security: Proactive Threat Detection for IoT Devices', ResearchGate. Available at: https://www.researchgate.net/profile/Floris-Huider-2/publication/389332767_AI-Powered_Information_Security_Proactive_Threat_Detection_for_IoT_Devices/links/67bee1b0461fb56424ea04aa/AI-Powered-Information-Security-Proactive-Threat-Detection-for-IoT-Devices.pdf (Accessed: 12 March 2025).

[76] Mitra, S., Chakraborty, T., Neupane, S. and Piplai, A. (2024) 'Use of graph neural networks in aiding defensive cyber operations', arXiv Preprint. DOI: 10.48550/arXiv.2401.05680 [Accessed 14 March 2025].

[77] Mitropoulou, K., Kokkinos, P. and Soumplis, P. (2024) 'Anomaly detection in cloud computing using knowledge graph embedding and machine learning mechanisms', Journal of Grid Computing, Springer. Available at: https://link.springer.com/article/10.1007/s10723-023-09727-1 [Accessed 14 March 2025].

[78] Moore, C. and Routhu, K. (2024) 'Leveraging Machine Learning Techniques for Predictive Analysis in Merger and Acquisition (M&A)', SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103189 (Accessed: 12 March 2025).

[79] Moorthy, S.K. and Jagannath, J. (2024) 'Survey of Graph Neural Network for Internet of Things and NextG Networks', arXiv. DOI: 10.48550/arXiv.2405.17309 (Accessed: 12 March 2025).

[80] Mupa, M.N, Tafirenyika, S., Nyajeka, M., Moyo, T., & Zhuwankinyu, K. (2025). Machine Learning in Actuarial Science: Enhancing Predictive Models for Insurance Risk Management. https://www.irejournals.com/formatedpaper/1707214.pdf

[81] Nagamani, G.M. and Kumar, C.K. (2024) 'Design of an improved graph-based model for real-time anomaly detection in healthcare using hybrid CNN-LSTM and federated learning', Heliyon. Available at: https://www.cell.com/heliyon/fulltext/S2405-8440(24)17102-2 (Accessed: 12 March 2025).

[82] Naghib, A., Gharehchopogh, F.S., and Zamanifar, A. (2025) 'A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities', SpringerLink. Available at: https://link.springer.com/article/10.1007/s10462-024-11101-w (Accessed: 12 March 2025).

[83] Nagpure, V. (2024) 'Case Study: The Next Generation of Network Management-AI, Automation, and Security in a Connected World', ResearchLake Journals. Available at: https://www.researchlakejournals.com/index.php/AAIML/article/view/379 (Accessed: 12 March 2025).

[84] Nagpure, V. (2024) 'Case Study: The Next Generation of Network Management-AI, Automation, and Security in a Connected World', ResearchLake Journals. Available at: https://www.researchlakejournals.com/index.php/AAIML/article/view/379 [Accessed 14 March 2025].

[85] Nagpure, V. (2024) Case Study: The Next Generation of Network Management - AI, Automation, and Security in a Connected World. ResearchLake Journals. Available at: https://www.researchlakejournals.com/index.php/AAIML/article/view/379 (Accessed: 12 March 2025).

[86] Nandan, M., Mitra, S. and De, D. (2025) 'GraphXAI: a survey of graph neural networks (GNNs) for explainable AI (XAI)', Neural Computing and Applications, Springer. Available at: https://link.springer.com/article/10.1007/s00521-025-11054-3 [Accessed 14 March 2025].

[87] Nguyen, H.T., Ngo, Q.D., and Le, V.H. (2020) 'A novel graph-based approach for IoT botnet detection', ResearchGate. Available at: https://www.researchgate.net/profile/Van-Hoang-Le-3/publication/336759151_A_novel_graph-based_approach_for_IoT_botnet_detection/links/61eb81f99a753545e2e9aec5/A-novel-graph-based-approach-for-IoT-botnet-detection.pdf (Accessed: 12 March 2025).

[88] Nguyen, H.X., Zhu, S. and Liu, M. (2022) 'A survey on graph neural networks for microservice-based cloud applications', Sensors, 22(23), Article 9492. DOI: 10.3390/s22239492 [Accessed 14 March 2025].

[89] Nguyen, H.X., Zhu, S. and Liu, M. (2022) 'A survey on graph neural networks for microservice-based cloud applications', Sensors, 22(23), Article 9492. DOI: 10.3390/s22239492 [Accessed 14 March 2025].

[90] NIST. (2021, July 12). AI Risk Management Framework | NIST. NIST. https://www.nist.gov/itl/ai-risk-management-framework

[91] Oliva delMoral, J. and deMarti iOlius, A. (2024) 'Cybersecurity in critical infrastructures: A post-quantum cryptography perspective', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10551387/ (Accessed: 12 March 2025).

[92] Paracha, M.A., Jamil, S.U., Shahzad, K., and Khan, M.A. (2024) 'Leveraging AI for network threat detection—a conceptual overview', Electronics, 13(23), Article 4611. DOI: 10.3390/electronics13234611 (Accessed: 12 March 2025).

[93] Patel, D., Raut, G., Cheetirala, S.N. and Nadkarni, G.N. (2024) 'Cloud Platforms for Developing Generative AI Solutions: A Scoping Review of Tools and Services', arXiv Preprint. DOI: 10.48550/arXiv.2412.06044 [Accessed 14 March 2025].

[94] Paul, A. L. (2024, May 30). The Role of Artificial Intelligence in Enhancing Data Security. ResearchGate; unknown. https://www.researchgate.net/publication/381004546_The_Role_of_Artificial_Intelligence_in_Enhancing_Data_Security

[95] Pauu, K.T., Wu, J., Fan, Y. and Pan, Q. (2023) 'Differential privacy and blockchain-empowered decentralized graph federated learning-enabled UAVs for disaster response', IEEE Xplore Conference Proceedings. Available at: https://ieeexplore.ieee.org/abstract/document/10315127/ [Accessed 14 March 2025].

[96] Porambage, P. and Liyanage, M. (2023) Security and Privacy Vision in 6G: A Comprehensive Guide. Available at: https://books.google.com/books?hl=en&lr=&id=Y-_NEAAAQBAJ&oi=fnd&pg=PR17&dq=gbsm+integration+with+blockchain-based+key+security+for+immutable+records&ots=VxuHVWbzm8&sig=TJWXVTINdSRsRMvLhdoAIK5Auc74 (Accessed: 12 March 2025).

[97] Prasad, V.K., Bhattacharya, P., Maru, D., and Tanwar, S. (2022) 'Federated learning for the internet-of-medical-things: A survey', MDPI Mathematics. DOI: 10.3390/math11010151 (Accessed: 12 March 2025).

[98] Qiu, Y., Huang, C., Wang, J., Huang, Z. and Xiao, J. (2022) 'A privacy-preserving subgraph-level federated graph neural network via differential privacy', Springer Lecture Notes in Computer Science. DOI: 10.1007/978-3-031-10989-8_14 [Accessed 14 March 2025].

[99] Rachid Ejjami. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. https://doi.org/10.70792/jngr5.0.v1i1.5

[100] Rahman, A. (2024) 'A Qualitative Study on The Reduction of Dwell Time Exceeding 200 Days', ProQuest Dissertations & Theses. Available at: https://search.proquest.com/openview/6f171f00e6f2033c2b106c09c8cb34c4/1?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 12 March 2025).

[101] Rallabandi, S. (2024) 'Autonomous Infrastructure Resilience: A Comparative Analysis Of AI-Driven Self-Healing Systems In Cloud Environments', arXiv. DOI: 10.48550/arXiv.2411.02093 (Accessed: 12 March 2025).

[102] Rallabandi, S. (2024) 'Autonomous Infrastructure Resilience: A Comparative Analysis Of AI-Driven Self-Healing Systems In Cloud Environments', International Journal of Cloud Engineering & Technology. DOI: 10.48550/arXiv.2411.02093 [Accessed 14 March 2025].

[103] Ramya, S., Smera, C. and Sandeep, J. (2025) 'Navigating Network Security: A Study on Contemporary Anomaly Detection Technologies', Wiley Online Library. DOI: 10.1002/9781394271429.ch11 [Accessed 14 March 2025].

[104] Rathore, M.M., Shah, S.A., Awad, A., and Shukla, D. (2021) 'A cyber-physical system and graph-based approach for transportation management in smart cities', Sustainability, 13(14), Article 7606. DOI: 10.3390/su13147606 (Accessed: 12 March 2025).

[105] Ravi, V., Pham, T.D., and Alazab, M. (2022) 'Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9863062/ (Accessed: 12 March 2025).

[106] Reddy, M., Konkimalla, S. and Rajaram, S.K. (2022) 'Using AI and machine learning to secure cloud networks: A modern approach to cybersecurity', SSRN Working Papers. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5045776 [Accessed 14 March 2025].

[107] Rehman, A. and Weng, J. (2025) 'Cyberattack Prevention Through AI-Powered Threat Detection and Response', ResearchGate. Available at: https://www.researchgate.net/profile/Jiefeng-Weng/publication/388848486_Cyberattack_Prevention_Through_AI-Powered_Threat_Detection_and_Response/links/67aa1f8b207c0c20fa837205/Cyberattack-Prevention-Through-AI-Powered-Threat-Detection-and-Response.pdf (Accessed: 12 March 2025).

[108] Rehman, S. and Ali, A. (2024) 'AI-Driven Identity and Access Management: Enhancing Authentication and Authorization Security', ResearchGate. Available at: https://www.researchgate.net/profile/Asif-Ali-136/publication/388525692_AI-Driven_Identity_and_Access_Management_Enhancing_Authentication_and_Authorization_Security/links/679bcc6e8311ce680c4471e5/AI-Driven-Identity-and-Access-Management-Enhancing-Authentication-and-Authorization-Security.pdf (Accessed: 12 March 2025).

[109] Rodrigues, P.D.C. de Sousa. (2019) 'An OSINT Approach to Automated Asset Discovery and Monitoring', ProQuest Dissertations & Theses. Available at: https://search.proquest.com/openview/762f9a1fd8c8694f231213065dadd16e/1?pq-origsite=gscholar&cbl=2026366&diss=y (Accessed: 12 March 2025).

[110] Ruzbahani, A.M. (2024) 'AI-Protected Blockchain-Based IoT Environments: Harnessing the Future of Network Security and Privacy', arXiv. DOI: 10.48550/arXiv.2405.13847 (Accessed: 12 March 2025).

[111] Salama, A.A., Shams, M.Y., and Bhatnagar, R. (2023) 'Optimizing Security Measures in Decentralized Mobile Networks with Neutrosophic Fuzzy Topology and PKI', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10389980/ (Accessed: 12 March 2025).

[112] Salem, S.A., Said, S.A., and Nour, S.M. (2024) 'AI-Driven Anomaly Detection Framework for Improving IoT System Reliability', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10833531/ (Accessed: 12 March 2025).

[113] Sangeetha, S.K.B., Selvarathi, C., and Mathivanan, S.K. (2024) 'Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Applications', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/10744551/ (Accessed: 12 March 2025).

[114] Shakhov, V. and Koo, I. (2021) 'Graph-based technique for survivability assessment and optimization of IoT applications', SpringerLink. Available at: https://link.springer.com/article/10.1007/s10009-020-00594-9 (Accessed: 12 March 2025).

[115] Sharma, S., Ramkumar, K.R., Kaur, A., and Hasija, T. (2023) 'Post-quantum cryptography: A solution to the challenges of classical encryption algorithms', SpringerLink. Available at: https://link.springer.com/chapter/10.1007/978-981-19-6383-4_3 (Accessed: 12 March 2025).

[116] Sindiramutty, S.R. and Prabagaran, K.R.V. (2025) 'Security Considerations in Generative AI for Web Applications', IGI Global. DOI: 10.4018/979-8-3693-5415-5.ch009 (Accessed: 12 March 2025).

[117] Singamaneni, K.K. and Muhammad, G. (2024) 'A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks', ScienceDirect. Available at: https://www.sciencedirect.com/science/article/pii/S157087052400218X (Accessed: 12 March 2025).

[118] Singh, A.K. and Siddiqui, A.A. (2024) 'Recent Advances in Computational Intelligence and Cyber Security', Taylor & Francis. Available at: https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.1201/9781003518587&type=googlepdf (Accessed: 12 March 2025).

[119] Singh, R., Khalid, S. and Nishad, D.K. (2024) 'Integrating Fuzzy Graph Theory into Cryptography: A Survey of Techniques and Security Applications', World Scientific, DOI: 10.1142/S179300572650016X (Accessed: 12 March 2025).

[120] Sood, N. (2024) 'Cryptography in post Quantum computing era', SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4705470 (Accessed: 12 March 2025).

[121] Sriram, H.K. (2022) 'AI Neural Networks In Credit Risk Assessment: Redefining Consumer Credit Monitoring And Fraud Protection Through Generative AI Techniques', Academia.edu. Available at: https://www.academia.edu/download/120988288/VOL_19_6_3.pdf (Accessed: 12 March 2025).

[122] Stufano, V.C. (2024) 'Esplorare le Capacità dei Large Language Models nell'Ottimizzare le Operazioni della Supply Chain', University of Genoa. Available at: http://unire.unige.it/handle/123456789/8294 (Accessed: 12 March 2025).

[123] Syed, N.F., Shah, S.W., Shaghaghi, A., and Anwar, A. (2022) 'Zero trust architecture (ZTA): A comprehensive survey', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9773102/ (Accessed: 12 March 2025).

[124] Tan, Y., Zhang, Q., Li, Y., and Yu, X. (2024) 'AI-Driven Network Security and Privacy', Electronics, 13(12), Article 2311. DOI: 10.3390/electronics13122311 (Accessed: 12 March 2025).

[125] Tan, Z., Parambath, S. P., Anagnostopoulos, C., Singer, J., & Marnerides, A. K. (2025). Advanced Persistent Threats Based on Supply Chain Vulnerabilities: Challenges, Solutions, and Future Directions. IEEE Internet of Things Journal, 12(6), 6371–6395. https://doi.org/10.1109/jiot.2025.3528744

[126] Tarafdar, R. (2024) AI-Powered Cybersecurity Threat Detection in Cloud Environments. ResearchGate. Available at: https://www.researchgate.net/profile/Research-Scholar-Ii/publication/389204120_AI-POWERED_CYBERSECURITY_THREAT_DETECTION_IN_CLOUD_ENVIRONMENTS/links/67b86523461fb56424e4e379/AI-POWERED-CYBERSECURITY-THREAT-DETECTION-IN-CLOUD-ENVIRONMENTS.pdf (Accessed: 12 March 2025).

[127] Thanalakshmi, P., Anitha, R., Anbazhagan, N., and Cho, W. (2021) 'A hash-based quantum-resistant chameleon signature scheme', Sensors, 21(24), Article 8417. DOI: 10.3390/s21248417 (Accessed: 12 March 2025).

[128] Tsoulias, K., Palaiokrassas, G., Fragkos, G. and Litke, A. (2020) 'A graph model-based blockchain implementation for increasing performance and security in decentralized ledger systems', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/9130718/ (Accessed: 12 March 2025).

[129] Ullah, B., Kamal, A., and Asif, S.A. (2024) 'Leveraging Artificial Intelligence for Advanced Cloud Security: Discussing Techniques and Applications', Coral Publications. DOI: 10.52633/4yjkrf74 (Accessed: 12 March 2025).

[130] Wajid, S. and Sans, M. (2024) 'Internet of Things Security: Leveraging AI and Machine Learning for Anomaly Detection', ResearchGate. Available at: https://www.researchgate.net/profile/Marta-Sans-2/publication/389350602_Internet_of_Things_Security_Leveraging_AI_and_Machine_Learning_for_Anomaly_Detection/links/67bf26238311ce680c75f925/Internet-of-Things-Security-Leveraging-AI-and-Machine-Learning-for-Anomaly-Detection.pdf (Accessed: 12 March 2025).

[131] Wan, C., Wang, Y., Xu, J., Wu, J., Zhang, T., and Wang, Y. (2024) 'Research on privacy protection in federated learning combining distillation defense and blockchain', Electronics, 13(4), Article 679. DOI: 10.3390/electronics13040679 (Accessed: 12 March 2025).

[132] Wen, S.F., Shukla, A., and Katt, B. (2025) 'Artificial intelligence for system security assurance: A systematic literature review', SpringerLink. Available at: https://link.springer.com/article/10.1007/s10207-024-00959-0 (Accessed: 12 March 2025).

[133] Wijenayake, D.S. and Henna, S. (2023) 'A Graph Neural Network-based Security Posture-aware Cloud Service Provider Selection for Multi-cloud', IEEE Xplore Conference Proceedings. Available at: https://ieeexplore.ieee.org/abstract/document/10470882/ [Accessed 14 March 2025].

[134] Wijenayake, D.S. and Henna, S. (2023) 'A Graph Neural Network-based Security Posture-aware Cloud Service Provider Selection for Multi-cloud', IEEE Xplore Conference Proceedings. Available at: https://ieeexplore.ieee.org/abstract/document/10470882/ [Accessed 14 March 2025].

[135] Win, T.Y., Tianfield, H., and Mair, Q. (2017) 'Big data-based security analytics for protecting virtualized infrastructures in cloud computing', IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/7949076/ (Accessed: 12 March 2025).

[136] Xin, R., Wang, J., Chen, P. and Zhao, Z. (2025) 'Trustworthy AI-based Performance Diagnosis Systems for Cloud Applications: A Review', ACM Computing Surveys. DOI: 10.1145/3701740 [Accessed 14 March 2025].

[137] Xu, R., Lan, Q., Pokhrel, S.R., and Li, G. (2023) 'A knowledge graph-based survey on distributed ledger technology for IoT verticals', ACM Digital Library. DOI: 10.1145/3609503 (Accessed: 12 March 2025).

[138] Xun, A.T., En, L.A.Z., Shen, L.T., Xin, A.N., Soon, W.H., and Jun, W.Z. (2025) 'Building Trust in Cloud Computing: Strategies for Resilient Security', Preprints.org. Available at:

https://www.preprints.org/frontend/manuscript/e07486fc39a494f2a9f999f253da8a79/download_pub (Accessed: 12 March 2025).

[139] Ye, M., Koteshwara, S., Dunn, D. and Franke, H. (2024) 'Position Paper: From Confidential Computing to Zero Trust, Come Along for the (Bumpy?) Ride', ACM Computing Surveys. DOI: 10.1145/3696843.3696848 [Accessed 14 March 2025].

[140] Ye, W., Qian, C., An, X. and Yan, X. (2023) 'Advancing federated learning in 6G: A trusted architecture with graph-based analysis', IEEE Xplore Conference Proceedings. Available at: https://ieeexplore.ieee.org/abstract/document/10436772/ [Accessed 14 March 2025].

[141] Zacharis, A., Katos, V., and Patsakis, C. (2024) 'Integrating AI-driven threat intelligence and forecasting in the cybersecurity exercise content generation lifecycle', SpringerLink. Available at: https://link.springer.com/article/10.1007/s10207-024-00860-w (Accessed: 12 March 2025).

[142] Zhang, C., Wang, N., Hou, Y.T., and Lou, W. (2024) 'Machine Learning-Based Intrusion Detection Systems: Capabilities, Methodologies, and Open Research Challenges', TechRxiv. Available at: http://www.techrxiv.org/doi/full/10.36227/techrxiv.173627464.48290242/v1 (Accessed: 12 March 2025).

[143] Zhang, K. (2023) 'Towards Data Privacy and Utility in the Applications of Graph Neural Networks', Georgia State University Dissertations. DOI: 10.57709/36369498 [Accessed 14 March 2025].

[144] Zhong, H., Yang, D., Shi, S., Wei, L. and Wang, Y. (2024) 'From data to insights: the application and challenges of knowledge graphs in intelligent audit', Springer Journal of Cloud Computing. Available at: https://link.springer.com/article/10.1186/s13677-024-00674-0 [Accessed 14 March 2025].

[145] Zhong, H., Yang, D., Shi, S., Wei, L. and Wang, Y. (2024) 'From data to insights: the application and challenges of knowledge graphs in intelligent audit', Journal of Cloud Computing, Springer. Available at: https://link.springer.com/article/10.1186/s13677-024-00674-0

[146] Zhuwankinyu, E., Moyo, S., Chivasa, C., & Ncube, S. (2023). E-Wild Life Alert: Tackling the Human-Wildlife Conflict Problem E-Wild Life Alert: Tackling the Human-Wildlife Conflict Problem. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1120&context=acist