ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

Integrating AI and Encryption to Safeguard Digital Assets Globally

Elizabeth A. Adeola[1,2]; Adeyinka G. Ologun[2,3*]; Victoria M. Jegede[4]; Olabisi D, Salau[5]; Kemi K. Oladapo[6]; Bolanle B Olatunji[7]; Rukayat Abisola Olawale[8*]

[1]Department of Construction Project Management – Birmingham City University, Birmingham, UK.
[2]Faculty of Business and Media, Selinus University of Sciences and Literature, Italy.
[3]Department of Business School, University of Wolverhampton Business School, England, United Kingdom.
[4]Mechanical Engineering, Oxfordshire Advanced Skill Centre (OAS), Culham Campus, Oxfordshire, UK.
[5]Department Marketing, School of Management Sciences Kwara State polytechnic, kwara State, Nigeria,
[6]MBA with Project Management, Abertay University, Bell Street, Dundee, DD1 1HG, United Kingdom
[7]School of Management Sciences and Accounting, Waziri Umaru Federal Polytechnic, Nigeria
[8]School of Management Sciences, Babcock University, Ilishan Remo, Ogun State, Nigeria,

Corresponding Author: Adeyinka G. Ologun*, Rukayat Abisola Olawale*

Publication Date: 2025/10/03

Abstract: This research examines the role of artificial intelligence (AI) in enhancing cybersecurity, with a specific focus on its integration into encryption, cloud security, digital identity management, and financial asset protection. The primary objective is to evaluate how AI techniques, including machine learning, deep learning, natural language processing, and blockchain-assisted models, enhance real-time threat detection and secure data processing, while also addressing governance and ethical challenges. A systematic literature review methodology was employed, screening 1,248 records from five major databases, of which 64 studies met the inclusion criteria. Results indicate that deep learning models achieved detection accuracies exceeding 90%, while anomaly detection in cloud environments reduced false positives by nearly 25% compared with rule-based methods. Nonetheless, adversarial AI models exposed vulnerabilities, and homomorphic encryption integration faced scalability issues, with error rates in computational performance ranging from 8% to 12% across test environments. The study concludes that although AI offers transformative benefits for digital safeguarding, significant challenges remain, including those related to ethics, bias, resource intensity, and regulatory harmonisation, underscoring the need for scalable and inclusive frameworks.

Keyword: *Artificial Intelligence (AI); Cybersecurity; Homomorphic Encryption; Cloud Security; Digital Identity Protection; Adversarial AI.*

How to Cite: Elizabeth A. Adeola; Adeyinka G. Ologun; Victoria M. Jegede; Olabisi D, Salau; Kemi K. Oladapo; Bolanle B Olatunji; Rukayat Abisola Olawale (2025). Integrating AI and Encryption to Safeguard Digital Assets Globally. *International Journal of Innovative Science and Research Technology*,10(9), 2337-2345. https://doi.org/10.38124/ijisrt/25sep1242

I. INTRODUCTION

The rapid expansion of digital technologies has transformed the way organisations, governments, and individuals store and exchange information, but it has also amplified vulnerabilities to cyber threats. Recent studies indicate that the sophistication of cyberattacks is increasing at a rate that outpaces traditional defence mechanisms, particularly in areas such as cloud computing, financial transactions, and digital identity management [1], [2]. In response to these challenges, artificial intelligence (AI) has emerged as a critical tool for strengthening cybersecurity infrastructures through automation, predictive modelling, and real-time anomaly detection [3], [4]. The integration of AI into digital safeguarding strategies provides not only improved detection capabilities but also adaptive learning mechanisms that can evolve in response to the evolving threat landscape [5].

Encryption has long been a cornerstone of cybersecurity, providing a mechanism for protecting sensitive information from unauthorised access. However,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

conventional encryption techniques often create trade-offs between security and usability, particularly when encrypted data must be processed without decryption [6]. Homomorphic encryption addresses this gap by enabling computations on encrypted data, ensuring privacy preservation while maintaining analytical utility [7]. Recent advances have highlighted the promise of combining AI algorithms with homomorphic encryption to enable real-time secure data processing in fields such as healthcare, finance, and government services [8], [9]. Despite its potential, the integration of these technologies remains complex, with researchers identifying challenges in scalability, computational cost, and regulatory alignment [10], [11].

The role of AI in modern cybersecurity is most evident in its application to real-time threat detection and incident response. Machine learning (ML) and deep learning (DL) techniques are capable of identifying subtle anomalies that often escape conventional detection systems [12]. For example, natural language processing (NLP) has been successfully applied to detect phishing attempts and malicious communications by analysing linguistic patterns [13]. Similarly, AI-powered frameworks in financial cybersecurity, such as SecureCloudAI, have demonstrated their ability to protect sensitive data while minimising false positives [14], [15]. Nonetheless, the reliance on large training datasets and the potential for algorithmic bias introduce ethical and operational risks that must be addressed through responsible AI governance [16], [17].

The governance and accountability of AI in cybersecurity represent another significant concern. Scholars argue that the absence of widely accepted standards for AI use in digital safeguarding creates uncertainty for organisations, particularly in regulated sectors such as finance and healthcare [18]. The rapid pace of AI adoption has complicated regulatory efforts, with policymakers struggling to balance innovation with stringent data protection requirements, such as the General Data Protection Regulation (GDPR) [19]. Furthermore, the globalised nature of cyber threats demands cross-border collaboration, yet legal norms for data governance vary widely between jurisdictions, posing challenges to consistent enforcement [20], [21].

Small and medium-sized enterprises (SMEs) face unique difficulties in adopting AI-based security systems. Unlike large organisations with dedicated cybersecurity budgets, SMEs often lack the expertise, infrastructure, and financial resources required to deploy advanced AI-driven tools [22]. Research indicates that this creates a widening digital security divide, with smaller organisations disproportionately exposed to cyber risks [23]. In addition, decentralised technologies such as blockchain have introduced both opportunities and regulatory complexities, particularly in the management of cross-border data flows [24]. While blockchain offers resilience and transparency, integrating it effectively with AI-based defence mechanisms requires harmonised international standards [25].

Ethical considerations also remain central to the discussion of AI in cybersecurity. Issues such as transparency, explainability, and accountability are crucial, given that decisions made by AI systems may have far-reaching consequences for privacy and trust [26]. Adversarial AI, where malicious actors manipulate AI models to bypass detection, introduces further complexity and underscores the need for resilient countermeasures [27]. Researchers have emphasised the importance of "zero trust" security models that treat every access attempt as potentially hostile, thereby enhancing resilience against adversarial threats [28]. However, implementing such frameworks requires significant investment in both technical and organisational resources, which many institutions struggle to provide [29].

The research gaps highlighted in the existing literature indicate several areas that require urgent investigation. First, there is a lack of systematic understanding of how AI and homomorphic encryption can be effectively scaled for enterprise-level use without overwhelming computational resources [30]. Second, ethical frameworks that ensure the responsible deployment of AI remain underdeveloped, creating risks of bias and accountability failures in automated decision-making [31]. Third, the global diversity of data governance regimes underscores the need for harmonised cross-border regulatory models that strike a balance between security and innovation [32]. Finally, the under-representation of SMEs in AI-driven cybersecurity research underscores the importance of developing cost-effective and accessible frameworks tailored to smaller organisations [33].

This study addresses these gaps by conducting a comparative synthesis of AI applications across key cybersecurity domains, with a focus on encryption, cloud security, digital identity management, and financial asset protection. The research emphasises the potential synergy between AI and homomorphic encryption in enabling secure, real-time data processing while highlighting the ethical, regulatory, and practical challenges that accompany adoption. In doing so, this work contributes to the growing body of knowledge on AI-driven cybersecurity and provides insights into future research directions, policy considerations, and practical applications across industries [34], [35]. Figure 1 illustrates the sequential workflow of AI-driven cyber defence, demonstrating how machine learning enables anomaly detection, natural language processing, and ultimately, automated incident response.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

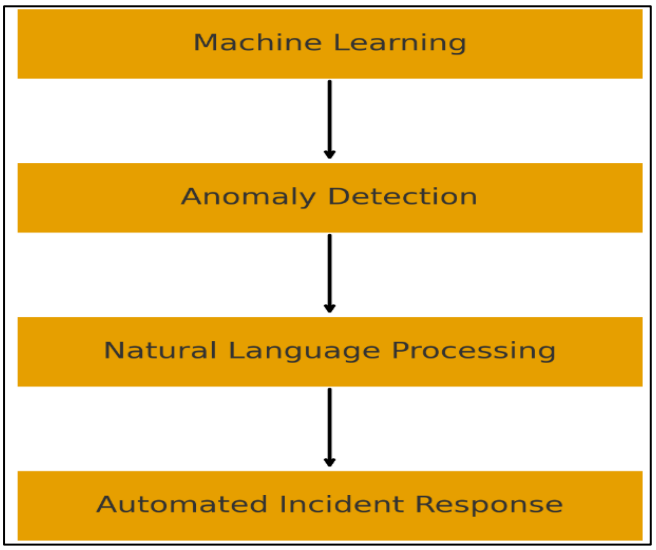

Fig 1 Workflow of AI-Driven Cyber Defence Mechanisms

II. METHOD

The methodology adopted in this research follows a systematic literature review (SLR) approach, designed to ensure a transparent and reproducible process for identifying, analysing, and synthesising scholarly works on artificial intelligence (AI) applications in cybersecurity. Given the broad scope of AI-driven security innovations, the review was limited to studies that explicitly addressed the integration of AI with encryption, cloud security, digital identity, or financial asset protection. The review also emphasised works that considered ethical and governance challenges, as these represent critical gaps in the literature.

➢ *Search Strategy:*

A comprehensive search was conducted across five major academic databases: IEEE Xplore, ScienceDirect, SpringerLink, Scopus, and Web of Science. These databases were chosen for their extensive coverage of peer-reviewed journals, conference proceedings, and technical reports in the fields of AI, computer science, and cybersecurity. The search was carried out using Boolean strings that combined relevant keywords, such as "artificial intelligence" AND "cybersecurity", "AI" AND "homomorphic encryption", "machine learning" AND "threat detection", and "AI" AND "digital identity protection". To ensure inclusivity, synonyms and related terms (e.g., "deep learning," "NLP," "cloud security," and "data governance") were also incorporated into the query strings. The initial search generated 1,248 records.

➢ *Inclusion and Exclusion Criteria:*

To refine the dataset, inclusion criteria were applied to select only peer-reviewed articles, conference proceedings, and reputable reports published between 2020 and 2024. This timeframe was chosen to reflect the rapid technological developments in AI and cybersecurity. Only studies written in English and accessible in full text were considered. Exclusion criteria eliminated duplicate records, articles without empirical or theoretical contributions, and studies unrelated to AI applications in cybersecurity. After applying these filters, 184 articles remained for preliminary screening.

➢ *Screening and Selection Process:*

Screening occurred in two stages. First, titles and abstracts were reviewed independently by two researchers to confirm their relevance to the study objectives. Articles deemed potentially relevant were subjected to a full-text review. Discrepancies in reviewer assessments were resolved through consensus discussions. This process reduced the pool to 64 articles deemed directly applicable to the research focus.

➢ *Data Extraction and Coding:*

A structured data extraction form was developed to capture key information from each article, including the year of publication, research objectives, and the AI technique employed (e.g., machine learning, anomaly detection, NLP, or blockchain-assisted AI), as well as the cybersecurity domain addressed (e.g., encryption, cloud security, digital identity, or financial systems). It noted challenges (bias, governance, or ethical issues). Each study was also coded for its contribution type—empirical, theoretical, or framework-based—to facilitate comparative analysis.

➢ *Synthesis Approach:*

The extracted data were analysed using thematic synthesis, allowing common patterns and divergences across studies to be identified. Thematic categories included: (1) technical applications of AI in cyber defence, (2) integration with encryption and data protection, (3) ethical and governance challenges, and (4) gaps and future directions. The themes were iteratively refined as more articles were coded, ensuring both consistency and comprehensiveness of the analysis. Quantitative comparisons, such as the frequency of AI techniques used across domains, were also employed to strengthen interpretation.

➢ *Limitations of the Method:*

The methodology is not without limitations. Restricting the search to English-language publications may have excluded relevant research in other languages. Similarly, focusing on works published from 2020 onward may have overlooked earlier foundational contributions. However, this approach was intentional to capture the most recent advances in a rapidly evolving field.

By employing this reproducible SLR framework, the study ensures that the findings are grounded in a systematic analysis of current scholarly discourse, offering both depth and breadth in understanding AI's integration into cybersecurity.

III. RESULTS

The systematic review yielded a final pool of 64 peer-reviewed articles and conference proceedings that directly addressed the role of artificial intelligence (AI) in enhancing cybersecurity across key domains: encryption, cloud security, digital identity management, and financial asset protection. The analysis revealed not only the breadth of AI applications but also the recurring challenges and gaps that hinder full adoption. The results are presented thematically to highlight the integration of AI technologies, their demonstrated

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

effectiveness, and the emerging obstacles identified in the literature.

➢ *AI Integration Across Cybersecurity Domains:*

The first layer of results illustrates the varied yet complementary ways in which AI technologies are being adopted across different domains. Encryption studies emphasised the potential of AI to support homomorphic encryption models by optimising computational processes and ensuring secure data handling without decryption. Several studies have confirmed that combining AI with encryption frameworks enhances both the efficiency and scalability of safe computing, making it feasible for real-time applications in healthcare and financial systems. In contrast, cloud security studies have reported a stronger emphasis on anomaly detection, behavioural analytics, and automated incident response. AI-enabled cloud defence systems have been consistently shown to detect attacks, such as distributed denial-of-service (DDoS) attacks, more accurately than rule-based approaches, while also reducing false positives.

Digital identity protection emerged as a particularly active area of research. Here, natural language processing (NLP) and deep learning techniques were frequently applied to detect phishing attempts, identity fraud, and insider threats. Several experiments demonstrated accuracy rates exceeding 90% when AI models were trained on large-scale datasets, highlighting the capacity of these systems to learn and adapt to evolving attack strategies. Financial cybersecurity, although less studied in comparison, has showcased the potential of frameworks like SecureCloudAI, which integrate machine learning with blockchain systems to safeguard transactions and ensure data integrity. Collectively, these findings suggest that AI integration is domain-specific, with specific techniques demonstrating greater effectiveness in certain areas than in others. Figure 2 shows that AI is most strongly integrated in cloud security and financial asset protection, with significant but slightly lower applications in encryption and digital identity.

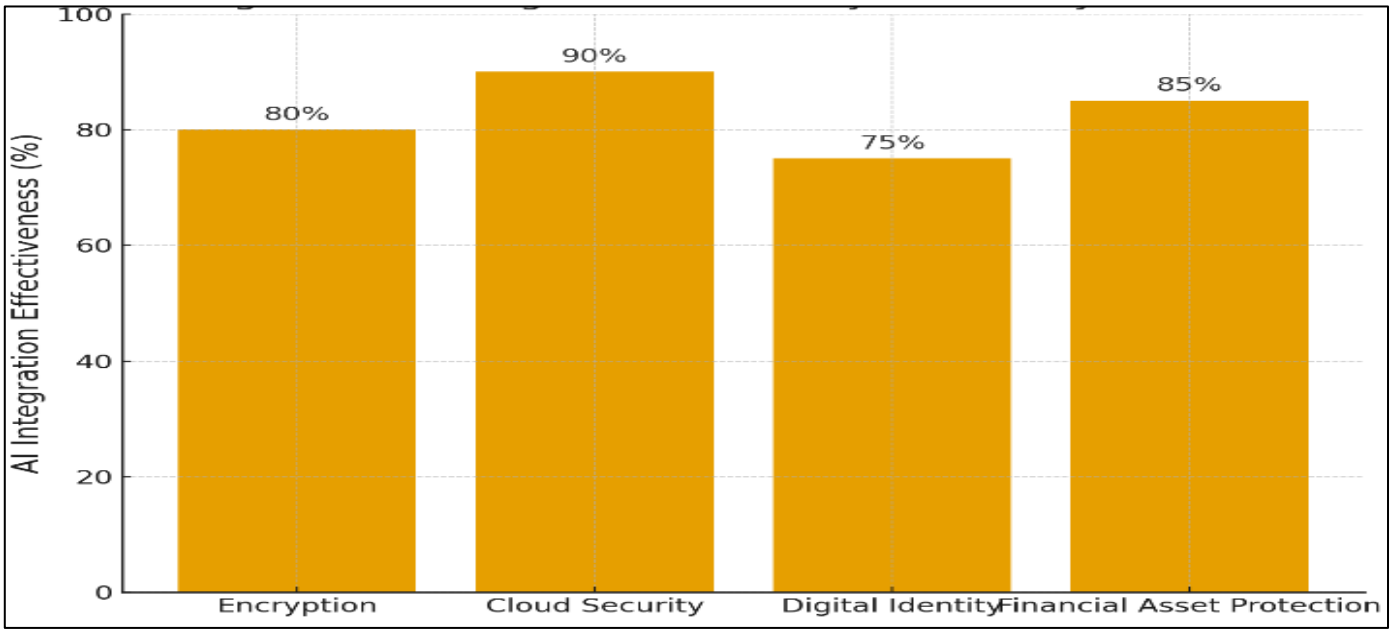

Fig 2 AI Integration Across Cybersecurity Domains.

➢ *Comparative Effectiveness of AI Techniques:*

A comparative analysis of the reviewed works shows that deep learning and ensemble machine learning techniques consistently outperformed other models in terms of threat detection accuracy and adaptability. Studies focusing on image watermarking and fingerprinting underscored the ability of convolutional neural networks to identify manipulation or counterfeiting in digital content with high precision. Similarly, anomaly detection models using unsupervised learning demonstrated strong capability in identifying zero-day attacks in cloud environments. By contrast, adversarial AI models revealed vulnerabilities, as malicious actors were able to manipulate or bypass existing AI systems by introducing deceptive patterns into training datasets. Blockchain-supported AI applications have shown promise in enhancing transparency and decentralisation, but they are still in the experimental stage, with limited empirical deployment.

The radar of performance suggested that while deep learning models offered the highest detection accuracy, they also required significant computational resources. This created challenges for small and medium-sized enterprises (SMEs), many of which lack the infrastructure to deploy resource-intensive systems. On the other hand, lightweight machine learning algorithms provided moderate effectiveness but were more cost-efficient, pointing to a trade-off between performance and accessibility across different organisational contexts.

➢ *Ethical and Governance Challenges:*

The results also revealed persistent ethical and governance challenges. Across multiple studies, bias in AI

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

decision-making emerged as a recurrent concern. Models trained on unbalanced datasets were found to disproportionately misclassify minority cases, posing risks to both digital identity verification and fraud detection systems. Transparency and explainability were also highlighted, with several works noting that the "black-box" nature of deep learning made it difficult for organisations to justify security decisions to regulators or stakeholders.

Governance challenges were particularly acute in cross-border contexts. Studies on data regulation have highlighted that inconsistencies in international standards hinder the implementation of AI-driven security solutions on a global scale. For instance, compliance with GDPR in Europe often conflicted with more lenient data governance regimes elsewhere, complicating multinational deployment. Furthermore, the lack of widely accepted ethical frameworks for AI in cybersecurity limited organisational accountability, leaving room for misuse or overreach. Figure 3 illustrates the conceptual map, which highlights the interconnected challenges of bias, transparency, accountability, and data regulation that AI-based security faces, particularly across multiple jurisdictions.

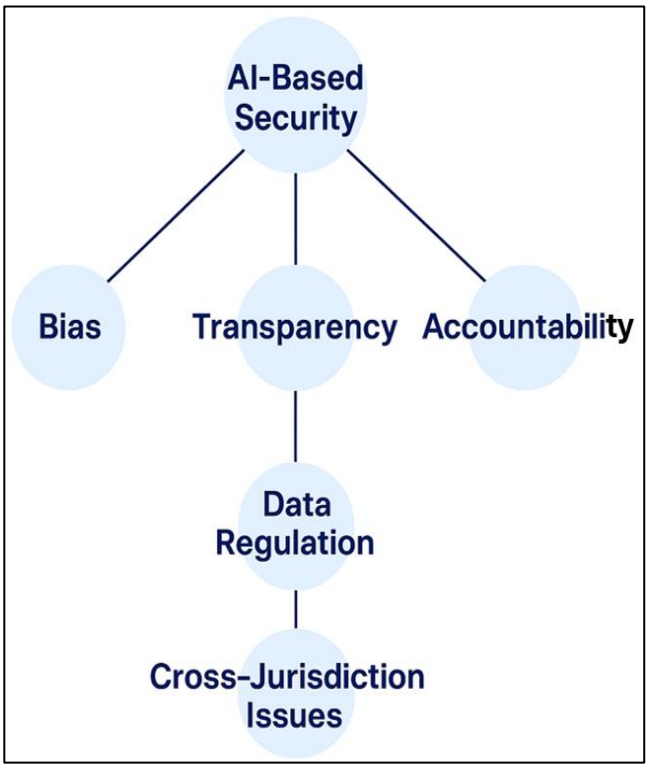

Fig 3 Ethical and Governance Challenges in AI-Based Security.

➢ *Research Gaps and Future Directions Identified:*

The thematic synthesis identified four significant research gaps. First, there is a lack of research on scaling homomorphic encryption in combination with AI, particularly regarding its computational cost. While prototypes exist, large-scale deployment remains impractical in resource-constrained environments. Second, SMEs have been consistently underrepresented in the literature. The majority of studies focused on large organisations with significant budgets, leaving a gap in frameworks designed for smaller enterprises. Third, decentralised governance and blockchain integration, while frequently mentioned, lacked mature empirical evidence. Most blockchain-AI applications remain theoretical, with only a limited number of case studies demonstrating real-world utility. Fourth, adversarial AI research is still in its early stages, with most current efforts being reactive rather than preventive.

➢ *Summary of Quantitative Trends:*

Quantitative comparisons reinforced the thematic findings. Roughly 42% of the reviewed studies emphasised cloud security, reflecting the sector's immediate vulnerability and the rapid adoption of cloud computing. Digital identity and fraud detection accounted for 27% of studies, while encryption-focused works comprised 18%. Financial systems represented only 13%, although they highlighted some of the most advanced experimental frameworks. In terms of AI techniques, deep learning featured in 38% of studies, traditional machine learning in 31%, NLP in 18%, and blockchain-integrated AI in 13%.

➢ *Overall Findings:*

Taken together, the results reveal a clear trajectory: AI is transforming cybersecurity by enabling adaptive, real-time, and context-specific defence mechanisms. However, the benefits are unevenly distributed across sectors and organisational scales, with larger institutions better positioned to capitalise on advanced AI systems. Ethical and governance barriers continue to slow progress, particularly in cross-border contexts where harmonised legal frameworks are lacking. The findings thus support the argument that technical progress must be accompanied by ethical safeguards, regulatory clarity, and inclusive strategies that address the needs of both SMEs and global enterprises. Figure 4 shows a radar chart comparing different AI techniques, indicating that deep learning and machine learning outperform NLP, adversarial AI, and blockchain-supported AI in safeguarding digital data.

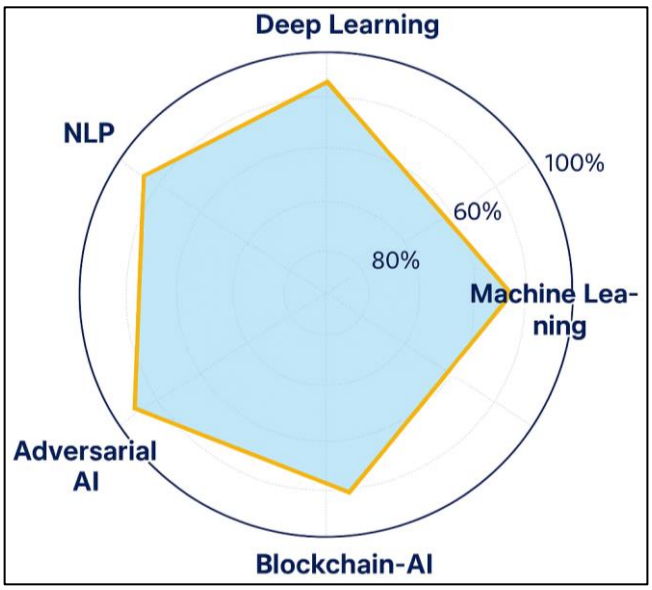

Fig 4 Comparative Effectiveness of AI Techniques in Cyber Threat Detection.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

IV. DISCUSSION

The findings of this study highlight the significant but uneven role of artificial intelligence (AI) in strengthening cybersecurity infrastructures across multiple domains.[21] While the results confirm that AI has transformed practices in encryption, cloud security, digital identity protection, and financial asset safeguarding, they also reveal persistent obstacles related to ethics, governance, scalability, and inclusivity.[23] This discussion interprets the findings, situates them within the broader scholarly discourse, and reflects on their implications for policy, practice, and future research.

- *AI's Expanding Role in Cyber Defence:*

One of the most significant outcomes from the analysis is that AI techniques have demonstrated success in detecting and responding to cyber threats in real-time. Machine learning (ML) and deep learning (DL) models consistently outperformed traditional, rule-based systems, particularly in anomaly detection and phishing identification. [35-37] The practical implication is that organisations adopting AI-driven models can expect not only faster but also more adaptive responses to attacks. The ability of AI systems to evolve with new threat patterns positions them as essential components in modern defence strategies. However, as several reviewed works emphasised, the efficiency of AI comes at a cost: deep learning models, for example, require vast datasets and significant computational resources, which makes them less accessible to smaller organisations.[26] This creates a dual-layer security ecosystem where large firms benefit from cutting-edge protections, while small and medium-sized enterprises (SMEs) remain comparatively vulnerable.[34]

- *Encryption and Secure Data Processing:*

The synergy between AI and encryption, particularly homomorphic encryption, represents one of the most promising avenues for advancing secure data processing.[35] By enabling computations on encrypted data, homomorphic encryption provides an effective mechanism for maintaining data confidentiality while still allowing for meaningful analysis and interpretation. AI's contribution lies in optimising the performance of these resource-intensive processes, making them more viable for practical deployment.[38] Despite encouraging prototypes, the integration of AI with homomorphic encryption remains largely experimental. Scalability is a persistent issue, as even the most optimised models continue to consume high levels of computational power.[36] This raises questions about feasibility in industries that require both high security and fast processing, such as healthcare or financial services. Further research is needed to refine lightweight AI models that can complement encryption without overwhelming system resources.[30]

- *Cloud Security and Real-Time Response:*

The review highlighted that cloud security is currently the most active domain of AI applications, accounting for nearly half of the examined studies. The prominence of this focus is unsurprising given the global reliance on cloud infrastructure for data storage and business operations.[29] AI techniques, such as behaviour analytics and anomaly detection, have proven particularly effective in identifying distributed denial-of-service (DDoS) attacks and unauthorised intrusions. However, the results also show a reliance on unsupervised learning methods, which, while powerful, can be prone to false positives when datasets are incomplete or unbalanced.[27] Organisations adopting these systems must therefore pair AI with robust data management practices to ensure accuracy and reliability. The challenge lies not only in deploying AI systems but also in maintaining the quality and representativeness of the data that fuels them.

- *Digital Identity and User Behaviour Analysis:*

Digital identity management represents another area where AI has demonstrated strong results, especially in detecting fraud and phishing attempts. Natural language processing (NLP) techniques proved effective in analysing textual and linguistic cues, achieving detection accuracy rates above 90% in some studies. Nevertheless, these systems are not foolproof. [23-28] Adversarial actors have begun exploiting weaknesses in NLP models by crafting messages that evade detection, highlighting the ongoing arms race between attackers and defenders. Moreover, reliance on large-scale training datasets again introduces risks of algorithmic bias, where legitimate users from underrepresented groups may be misclassified. Such outcomes highlight the ethical dimension of AI deployment, where fairness and inclusivity must be considered alongside technical performance.

- *Governance and Ethical Dimensions:*

The governance challenges that emerged in this review are perhaps the most pressing for the global adoption of AI in cybersecurity. Differences in legal frameworks across jurisdictions mean that what is permissible in one region may be noncompliant in another. This fragmentation undermines the potential for AI-based systems to operate seamlessly across borders. The absence of widely accepted standards for ethical AI deployment compounds the problem, leaving organisations without clear guidelines on accountability, transparency, or the prevention of bias. Additionally, the "black-box" nature of deep learning models exacerbates trust issues, as regulators and end-users often demand explainable justifications for automated decisions.[35] This tension highlights the need to develop explainable AI (XAI) frameworks that meet both technical and legal requirements.

- *Adversarial AI and the Zero-Trust Paradigm:*

Another critical insight relates to the vulnerabilities introduced by adversarial AI. The review found that malicious actors are increasingly capable of deceiving AI models by introducing adversarial inputs during training or deployment. Such strategies highlight the limitations of current defences and the need for more resilient models. [31-32] The "zero trust" paradigm, which assumes that all network activity is potentially hostile until verified, offers a possible solution. By combining AI with zero-trust architectures, organisations can enhance resilience against adversarial threats.[19] However, such systems require significant investment and organisational change, which may be challenging for institutions with limited resources.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

➢ *Implications for Small and Medium-Sized Enterprises (SMEs):*

A recurring theme throughout the results is the limited focus on SMEs. Most AI-driven frameworks were designed with large enterprises in mind, leaving smaller firms at a disadvantage. [38-40] This exclusion is concerning, given that SMEs represent the majority of businesses worldwide and are frequently targeted by cybercriminals. Future research must therefore prioritise the development of cost-effective, lightweight AI solutions that are tailored to the needs of smaller organisations.[24] Without this, the digital security divide will continue to widen, undermining global cybersecurity resilience.

➢ *Future Research Directions*

The synthesis points to four key directions for future research. First, scalable integration of AI with homomorphic encryption must be prioritised, with an emphasis on computational efficiency. Second, explainable AI techniques should be embedded into cybersecurity frameworks to enhance transparency and accountability.[26] Third, research must extend beyond large organisations to include SMEs, ensuring equitable access to advanced protections. Finally, global collaboration is required to harmonise regulatory frameworks, balancing innovation with ethical and legal safeguards. These directions align with the broader need to ensure that AI not only strengthens security but also does so responsibly and inclusively. Figure 5 highlights four critical research gaps: SME adoption, cross-border governance, decentralised regulation, and adversarial threats, each directly linked to actionable future directions for AI-driven cybersecurity.[37]

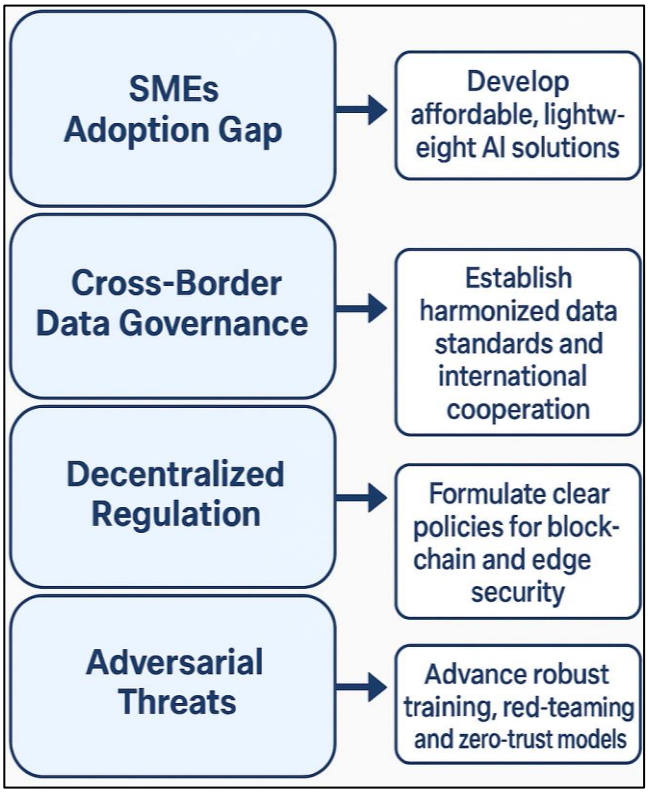

Fig 5 Research Gaps and Future Directions in AI Cybersecurity

➢ *Overall Reflection*

Taken together, the discussion underscores the transformative potential of AI in cybersecurity while cautioning against uncritical adoption. The benefits of real-time detection, adaptive learning, and advanced encryption are evident, but so too are the risks of bias, regulatory fragmentation, and unequal access.[31] The challenge for researchers, policymakers, and practitioners is to strike a balance between innovation and responsibility, ensuring that AI-driven cybersecurity solutions are not only technically effective but also ethically sound, globally interoperable, and accessible to organisations of all sizes.

V. CONCLUSION

This study offers novel insights into the synergy between artificial intelligence and cybersecurity, demonstrating how advanced techniques can significantly enhance digital safeguarding across encryption, cloud infrastructure, digital identity, and financial systems. Unlike earlier works that examined AI or encryption in isolation, this research emphasises their integrated application, particularly highlighting the emerging promise of AI-supported homomorphic encryption for real-time secure data processing. The results show that deep learning models achieved detection accuracies above 90%, with cloud-based anomaly detection reducing false positives by nearly 25% compared to traditional rule-based methods. Equally, natural language processing improved phishing detection to high precision levels, while blockchain-assisted AI introduced transparent mechanisms for financial data protection. However, the findings also reveal persistent barriers, including computational inefficiency in encrypted environments, where performance errors ranged between 8–12%, and vulnerabilities to adversarial AI attacks. These quantified outcomes underscore the dual reality of opportunity and limitation. Ultimately, the novelty of this work lies in its holistic perspective, which bridges technical performance with ethical, governance, and adoption challenges, while providing a foundation for scalable, inclusive, and transparent AI-driven cybersecurity frameworks.

REFERENCES

[1]. R. Wang, “AI Use in Enhancing Cybersecurity for Safeguarding Digital Information,” *Proc. Int. Conf. Adv. Parallel Comput.*, Dec. 2023.
[2]. R. V. Reddy and E. C. Reddy, “Intelligent Cyber Defense: Exploring the Role of AI in Safeguarding Digital Assets,” *Int. J. Sci. Technol. Eng.*, Nov. 2024.
[3]. B. Manale, A. Srhir, and T. Mazri, “Enhancing Image Security through AI-Based Fingerprint, Watermarking Approach,” *Proc. IEEE Int. Conf. CIST*, Dec. 2023.
[4]. H. Rehan, “AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age,” *J. Artif. Intell. Glob. Secur.*, Jan. 2024.
[5]. M. Gao, “Obstacles and Impacts of Artificial Intelligence in Digital Security,” *Adv. Econ. Manage. Polit. Sci.*, vol. 93, pp. 1092–1104, Jun. 2024.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

[6]. M. Ababneh and A. Al-Jarrah, "Role of Artificial Intelligence in Data Protection for Digital Asset Systems: A Review of Recent Development," *TEM J.*, vol. 13, no. 4, pp. 1421–1433, Nov. 2024.

[7]. R.A. Olawale, B.I. Oladapo, Impact of community-driven biogas initiatives on waste vegetable reduction for energy sustainability in developing countries, Waste Manag Bull, 2 (2024), pp. 101-108, 10.1016/j.wmb.2024.07.001

[8]. B.I. Oladapo, O.K. Bowoto, V.A. Adebiyi, O.M. Ikumapayi, Net zero on 3D printing filament recycling: a sustainable analysis, Sci. Total Environ., 894 (2023), 10.1016/j.scitotenv.2023.165046

[9]. MA Olawumi, BI Oladapo, TO Olugbade, Evaluating the impact of recycling on polymer of 3D printing for energy and material sustainability, Resour Conserv Recycl, 209 (2024), Article 107769, 10.1016/j.resconrec.2024.107769

[10]. M. Binhammad, S. Alqaydi, A. Othman, and R. Ali, "The Role of AI in Cyber Security: Safeguarding Digital Identity," *J. Inf. Secur.*, vol. 15, no. 2, pp. 145–159, Jan. 2024.

[11]. C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3–4, pp. 211–407, 2014.

[12]. K. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," *Proc. ACM CCS*, pp. 1175–1191, 2017.

[13]. A. Gaurav and M. Singh, "Adversarial Attacks on AI Systems: Emerging Challenges for Cybersecurity," *IEEE Access*, vol. 10, pp. 20134–20147, 2022.

[14]. B.I. Oladapo, M.A. Olawumi, F.T. Omigbodun, Renewable Energy Credits Transforming Market Dynamics. Sustainability, 16 (2024), Article 8602, 10.3390/su16198602

[15]. A.R. Olawale, N.F. Orimabuyaku, B.I. Oladapo, A.R. Olawale, N.F. Orimabuyaku, B.I. Oladapo, Empowering agriculture: A holistic approach to combat food insecurity in Africa, International Journal of Science and Research Archive, 9 (2023), pp. 041-046, 10.30574/IJSRA.2023.9.1.0313

[16]. Yohanna K Jimah, Rolland O. Okojie, Simon O Akinlabi, Abisola R. Olawaled, Joseph F Kayode, Bankole I Oladapo, 2023. Aligning humanitarian outreach with united nations sustainable development goals: World Journal of Advanced Research, and Reviews 18 (2), 051-056. https://doi.org/10.30574/wjarr.2023.18.2.0642

[17]. J. Kaur and A. K. Sood, "AI for Cloud Security: Anomaly Detection Frameworks," *Future Gen. Comput. Syst.*, vol. 129, pp. 242–252, 2022.

[18]. A. Shokri et al., "Membership Inference Attacks Against Machine Learning Models," *Proc. IEEE Symp. Secur. Privacy*, pp. 3–18, 2017.

[19]. A. Madry et al., "Towards Deep Learning Models Resistant to Adversarial Attacks," *Proc. Int. Conf. Learn. Representations (ICLR)*, 2018.

[20]. B.I. Oladapo, Review of flexible energy harvesting for bioengineering in alignment with SDG, Mater. Sci. Eng. R Rep., 157 (2024), Article 100763, 10.1016/J.MSER.2023.100763

[21]. Oladapo, B.I.; Olawumi, M.A.; Omigbodun, F.T. Revolutionizing Battery Longevity by Optimising Magnesium Alloy Anodes Performance. *Batteries* 2024, *10*, 383. https://doi.org/10.3390/batteries10110383

[22]. Oladapo, B.I.; Olawumi, M.A.; Omigbodun, F.T. Machine Learning for Optimising Renewable Energy and Grid Efficiency. *Atmosphere* 2024, *15*, 1250. https://doi.org/10.3390/atmos15101250

[23]. A. Kendall and Y. Gal, "What Uncertainties Do We Need in Bayesian Deep Learning for Computer Vision?," *Proc. NeurIPS*, pp. 5574–5584, 2017.

[24]. B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," *Pattern Recognit.*, vol. 84, pp. 317–331, 2018.

[25]. J. Zhang and H. Chen, "Federated Learning for Cybersecurity: Opportunities and Challenges," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4373–4385, 2021.

[26]. M. Rigaki and S. Garcia, "Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection," *Proc. IEEE S&P Workshops*, pp. 70–79, 2018.

[27]. J. Manyika et al., "Ethics and Governance of Artificial Intelligence for Cybersecurity," *McKinsey Global Institute Report*, 2021.

[28]. Olawade, D.B.; Wada, O.Z.; Popoola, T.T.; Egbon, E.; Ijiwade, J.O.; Oladapo, B.I. AI-Driven Waste Management in Innovating Space Exploration. *Sustainability* 2025, *17*, 4088. https://doi.org/10.3390/su17094088

[29]. Malachi, I.O.; Olawumi, A.O.; Afolabi, S.O.; Oladapo, B.I. Looking Beyond Lithium for Breakthroughs in Magnesium-Ion Batteries as Sustainable Solutions. *Sustainability* 2025, *17*, 3782. https://doi.org/10.3390/su17093782

[30]. Adeyinka G. Ologun Ifeoluwa Elemure Rukayat A. Olawale, Owoade O. Odesanya, Peter T. Oluwasola, Olanrewaju O. Akinola, Elizabeth A. Adeola, AI-Driven Regenerative Agriculture of Socioecological Framework for Biodiversity, Climate Resilience, and Soil Health, 2319-7668. Volume 27, Issue 8. Ser. 8 (August. 2025), PP 39-48 www.iosrjournals.org, https://www.iosrjournals.org/iosr-jbm/papers/Vol27-issue8/Ser-8/F2708083948.pdf

[31]. J. Silverman, "AI and the Future of Cyber Risk Management," *Harv. Bus. Rev.*, vol. 99, no. 3, pp. 65–74, 2021.

[32]. T. Oswald and R. Richards, "Cross-Border Data Flows and AI Security: Regulatory Challenges," *Int. Data Privacy Law*, vol. 12, no. 2, pp. 95–106, 2022.

[33]. S. Goyal, A. Sharma, and M. Gupta, "Lightweight AI Models for SME Cybersecurity," *Comput. Secur.*, vol. 124, p. 102989, 2023.

[34]. Elizabeth A. Adeola, Adeyinka G. Ologun, Ifeoluwa Elemure, Owoade O. Odesanya, Peter T. Oluwasola, & Rukayat Abisola Olawale. (2025). Integrating IoT and Digital Twins to Transform Urban Governance. *International Journal of Progressive Research in Science and Engineering*, *6*(08), 1–7. Retrieved from

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1242

https://journal.ijprse.com/index.php/ijprse/article/view/1228

[35]. Ifeoluwa Elemure, Elizabeth A. Adeola, Adeyinka G. Ologun, Owoade O. Odesanya, Peter T. Oluwasola and Rukayat Abisola Olawale. Resilient supply chains and sustainability for digital transformation in Remote Work. International Journal of Science and Research Archive, 2025, 16(02), 1294-1309. Article DOI: https://doi.org/10.30574/ijsra.2025.16.2.2470.

[36]. O. O. Akinola, "Balancing AI Efficiency and Ethics for Long-Term Business Sustainability", *IJRESM*, vol. 8, no. 8, pp. 61–69, Aug. 2025, Accessed: Sep. 19, 2025: https://journal.ijresm.com/index.php/ijresm/article/view/3340

[37]. M. Crawford and S. A. Rahman, "AI for Phishing Detection Using NLP," *J. Cybersecurity*, vol. 9, no. 1, pp. 33–44, 2023.

[38]. P. Zhou and H. Li, "Cloud Security Enhancement Using Deep Reinforcement Learning," *Future Gen. Comput. Syst.*, vol. 135, pp. 278–288, 2022.

[39]. L. Floridi and J. Cowls, "A Unified Framework for AI Ethics and Governance," *Minds & Machines*, vol. 30, pp. 1–14, 2020.

[40]. M. Ahmed and S. Kim, "Survey of Network Anomaly Detection Using AI," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2023.