World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Research Article)

Federated learning for privacy-preserving data analytics in mobile applications

Joy Nnenna Okolo [1, *], Adesola Abdul-Gafar Arowogbadamu [2], Samuel A. Adeniji [3] and Rhoda Kalu Tasie [4]

[1] McComish Department of Electrical Engineering and Computer Science, South Dakota State University, Brookings, South Dakota, United States.
[2] Department of Management and Accounting, Obafemi Awolowo University, Ile-Ife, Osun State, Nigeria.
[3] Department of Computer and Information Science, Western Illinois University, Macomb, Illinois, United States.
[4] Department of Industrial Engineering, University of Arkansas, Fayetteville, Arkansas, United States.

World Journal of Advanced Research and Reviews, 2025, 26(01), 1220-1232

Publication history: Received on 24 February 2025; revised on 07 April 2025; accepted on 09 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1099

Abstract

The rapid adoption of mobile AI applications in areas such as healthcare, finance, and personalized services has raised significant concerns about data privacy and security. Traditional centralized machine learning (ML) models require mobile devices to transmit user data to cloud servers, posing risks of data breaches and regulatory non-compliance. Federated learning (FL) addresses these concerns by allowing decentralized AI model training directly on user devices, ensuring that raw data remains private and never leaves the device. However, FL faces security vulnerabilities and performance limitations, including model inversion attacks, data poisoning risks, and high computational overhead. This paper explores key privacy-preserving techniques such as differential privacy, secure aggregation, and homomorphic encryption, which enhance FL security while maintaining model accuracy. Additionally, emerging trends such as blockchain-integrated FL, post-quantum cryptography, and AI-driven optimization are analyzed to highlight the future of privacy-preserving mobile AI ecosystems. By integrating advanced cryptographic techniques and decentralized verification mechanisms, FL can enable scalable, secure, and regulation-compliant AI applications, ensuring a balance between data privacy and AI innovation.

Keywords: Federated Learning; Privacy-Preserving AI; Mobile Data Security; Differential Privacy; Blockchain-Based FL

1. Introduction

The rapid expansion of mobile applications in industries such as health care, finance, social media, and personalized AI services has significantly increased concerns about user data privacy and security [39,92].Traditional centralized machine learning (ML) models require mobile applications to upload user data to cloud servers for processing, posing risks of data breaches, unauthorized access, and regulatory violations[28].Additionally, with stricter data protection laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), organizations must adopt privacy-preserving AI techniques to ensure that mobile applications handle user data securely and ethically. In response to these challenges, federated learning (FL) has emerged as a transformative approach, allowing AI models to be trained directly on users' mobile devices without sharing raw data with a central server [78].

Federated learning offers a decentralized approach to AI training, reducing the reliance on cloud computing while minimizing privacy risks. Unlike traditional ML, which requires data to be collected, transmitted, and stored in centralized data centers, FL enables mobile devices to collaboratively train models locally while only sharing encrypted model updates with a central aggregator [26]. This approach ensures that sensitive user information remains on the device, preventing exposure to potential cyber threats and data leaks. Additionally, FL is particularly beneficial in

[*] Corresponding author: Joy Nnenna Okolo.

privacy-sensitive applications such as mobile health tracking, personalized recommendations, and financial fraud detection, where preserving user confidentiality is critical [7].

Beyond privacy protection, federated learning also enhances real-time AI personalization without compromising data security [45].By processing data directly on mobile devices, FL enables applications to adapt to user preferences more efficiently, improving the performance of voice assistants, predictive keyboards, and recommendation systems[21].This decentralized approach also reduces cloud dependency, leading to lower latency, improved bandwidth efficiency, and cost savings for mobile service providers. As a result, major tech companies such as Google, Apple, and Meta have already adopted FL in applications like Gboard, Siri, and Meta's AI assistants to provide privacy-preserving user experiences [9]. However, despite its advantages, federated learning comes with several technical and security challenges. The distributed nature of FL introduces computational and energy constraints, as mobile devices have limited processing power and battery life compared to cloud data centers [3]. Additionally, FL is vulnerable to adversarial attacks, including model poisoning, data inversion, and inference attacks, where malicious entities attempt to manipulate FL training processes or extract private user information from shared model updates [56]. Ensuring the security and integrity of FL-based AI models requires the integration of advanced privacy-preserving techniques, such as differential privacy, secure aggregation, and homomorphic encryption [30].

Another key challenge is ensuring regulatory compliance and cross-border data privacy in federated learning implementations [52]. While FL reduces the risk of centralized data breaches, mobile applications must still comply with regional privacy laws and industry-specific regulations governing data access, storage, and processing [24]. Moreover, federated learning model updates still carry metadata and statistical information that could be exploited if not properly protected. Addressing these concerns requires continuous advancements in cryptographic techniques, secure model update aggregation, and privacy-aware AI governance frameworks to ensure that FL remains a trustworthy and scalable solution for mobile applications [65].

This paper explores federated learning as a privacy-preserving AI approach for mobile applications, discussing key security techniques, including differential privacy, secure aggregation, and homomorphic encryption [49]. Additionally, it examines the challenges of implementing FL in mobile environments, such as scalability issues, security risks, and regulatory compliance hurdles [11,93]. The paper also highlights future trends in FL, including blockchain-based model verification, post-quantum cryptography, and AI-driven compliance automation, which will shape the next generation of secure and privacy-preserving mobile AI systems [73].

2. Material and Methods

This study adopts a conceptual research approach, focusing on a comprehensive review and comparative analysis of existing literature on federated learning (FL) techniques and their application in privacy-preserving mobile AI systems. The objective was to identify and evaluate key privacy-enhancing mechanisms, implementation challenges, and emerging trends in FL deployments across mobile platforms.

2.1. Literature Review Strategy

Relevant academic and industry publications were sourced from reputable databases, including IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. Search keywords included combinations of terms such as *"federated learning," "mobile applications," "privacy-preserving AI," "differential privacy," "secure aggregation," "homomorphic encryption,"* and *"blockchain-based federated learning."* The search was limited to articles published between 2015 and 2024 to ensure that only current and relevant research was included.

2.2. Inclusion and Exclusion Criteria

Articles were selected based on their relevance to federated learning in mobile environments, with particular emphasis on privacy, security, cryptographic techniques, and compliance with data protection regulations. Studies that focused solely on cloud-based AI or non-mobile implementations were excluded unless they provided transferable insights applicable to mobile FL contexts.

2.3. Analytical Framework

The selected studies were organized into thematic categories based on the primary privacy-preserving technique discussed—namely, differential privacy, secure aggregation, and homomorphic encryption. These categories were then analyzed for their technical mechanisms, real-world applicability, computational trade-offs, and regulatory compliance.

The paper also presents a comparative analysis table to synthesize the strengths and weaknesses of these techniques and identify their best use cases in mobile AI.

This structured, qualitative method allowed the study to identify critical gaps, emerging solutions, and practical recommendations for advancing secure, decentralized AI through federated learning in mobile ecosystems.

3. Results and Discussion

3.1. Differential Privacy for Secure FL Model Training

Differential privacy (DP) is a privacy-preserving technique that enhances federated learning (FL) security by adding mathematical noise to local model updates before they are shared with the central aggregator [27]. In traditional FL, mobile devices train AI models on decentralized data and send their updates to a central server for aggregation. However, even without direct access to raw data, adversaries can still infer sensitive user information from model updates through techniques such as model inversion or membership inference attacks [17]. Differential privacy mitigates this risk by introducing randomized noise to each model update, ensuring that no single data point can be distinguished or reconstructed, thereby protecting individual user identities [89].

One of the key strengths of differential privacy is that it provides provable privacy guarantees by making it mathematically impossible to trace AI model updates back to specific users [91]. This is particularly valuable in mobile applications where users generate highly sensitive data, such as health metrics, location history, and financial transactions. By integrating DP into FL, mobile applications can train AI models on personalized user data while ensuring compliance with privacy regulations such as GDPR, HIPAA, and CCPA [55]. Additionally, DP prevents insider threats, as even service providers hosting the FL framework cannot extract identifiable information from aggregated models. This makes DP-enhanced FL particularly effective for secure AI-driven applications like personalized healthcare monitoring, voice assistants, and mobile recommendation systems [14].

Despite its privacy benefits, differential privacy introduces challenges related to model accuracy. The noise added to model updates can reduce the precision of AI predictions, particularly if the privacy budget (ε-value) is set too low, prioritizing stronger privacy guarantees over model performance [27]. In mobile health analytics, for example, an excessively noisy AI model may struggle to provide accurate disease risk assessments or personalized health recommendations [61]. To address this trade-off, researchers are developing adaptive DP mechanisms, where the level of noise dynamically adjusts based on data sensitivity and AI task complexity, ensuring a balance between privacy protection and AI model reliability [85].

A major use case for differential privacy in FL is privacy-preserving mobile health analytics and personalized AI assistants [69]. Mobile health applications, such as wearable fitness trackers and remote patient monitoring systems, collect highly sensitive medical data that must remain confidential. By leveraging DP-enhanced FL, these applications can train AI models to detect health anomalies, recommend personalized workouts, or predict disease risks, all while ensuring that individual user data is never directly exposed [83]. Similarly, DP can enhance personalized AI assistants (e.g., Siri, Google Assistant), allowing them to learn from user interactions without storing identifiable voice patterns or behavioral data on central servers. As privacy regulations tighten, differential privacy will play a crucial role in securing federated learning models, ensuring that mobile AI applications remain both intelligent and privacy-compliant [70,94].

3.2. Secure Aggregation for FL Model Updates

Secure aggregation is a cryptographic technique designed to encrypt model updates in federated learning (FL) before they are sent to the central server, ensuring that no single party—including the aggregator—can access individual device updates [29]. In standard FL, mobile devices train AI models locally and transmit their updates for aggregation, but these updates can still leak sensitive information if intercepted by attackers or compromised by malicious entities [12]. Secure aggregation addresses this risk by enabling privacy-preserving model training, where only the final aggregated model is accessible, while individual contributions remain encrypted and confidential. This ensures that even if an attacker gains access to the central server, they cannot extract user-specific insights from model updates, significantly enhancing FL security [3].

One of the main strengths of secure aggregation is that it prevents data leakage during FL training by ensuring that model updates remain private, even in the presence of an untrusted server [66]. This is particularly important for privacy-sensitive mobile applications, where users generate highly confidential data, such as financial transactions, biometric authentication patterns, and personal spending behaviours [1]. Secure aggregation also aligns with global data protection regulations, such as GDPR, HIPAA, and PSD2, by ensuring that mobile applications can train AI models on decentralized user data without violating privacy policies. Furthermore, secure aggregation strengthens resilience against adversarial attacks, reducing the risk of membership inference or model inversion attacks, where attackers attempt to reconstruct original training data [38].However, secure aggregation introduces computational and efficiency challenges, particularly for resource-constrained mobile devices [46].Encrypting each model update before transmission increases computational overhead, leading to higher energy consumption, increased latency, and slower AI model training[2]. Additionally, implementing multi-party cryptographic techniques, such as homomorphic encryption or secure multiparty computation (SMPC), adds complexity to key management and decryption processes. These limitations make it difficult to apply secure aggregation in real-time mobile AI applications, where low latency and minimal power consumption are critical. To mitigate these challenges, researchers are exploring lightweight encryption techniques and optimized cryptographic protocols, ensuring that secure aggregation can be efficiently deployed in large-scale mobile FL networks [79].

A major use case for secure aggregation in federated learning is financial mobile applications that process sensitive transaction data. Banking apps, mobile payment platforms, and fraud detection systems require strong privacy guarantees to protect customer financial records, transaction histories, and behavioral spending patterns[50].By integrating secure aggregation into FL-based financial AI models, banks and FinTech companies can collaboratively train fraud detection systems across multiple institutions without exposing individual customer data[60].This allows financial organizations to detect emerging fraud patterns while maintaining compliance with banking regulations, ensuring that users' financial data remains private, secure, and decentralized [64].

3.3. Homomorphic Encryption for Fully Secure FL Processing

Homomorphic encryption (HE) is a cryptographic technique that enables computation on encrypted data without requiring decryption, ensuring end-to-end privacy in federated learning (FL) [86]. In traditional FL, model updates from mobile devices are aggregated centrally, but even encrypted updates can sometimes leak sensitive information through statistical inference attacks. HE eliminates this risk by allowing mobile devices to encrypt their model updates before transmission and enabling the central aggregator to perform computations directly on the encrypted data [17]. This ensures that even if the server is compromised, attackers cannot extract any meaningful information from intercepted model updates, making HE one of the most secure privacy-preserving techniques for FL [87].

A key strength of homomorphic encryption in FL is its ability to provide uncompromised data privacy, ensuring that no raw data or model updates are exposed at any stage of processing [43]. This makes HE particularly valuable for highly sensitive mobile applications, such as healthcare analytics, financial fraud detection, and biometric authentication systems, where user data confidentiality is non-negotiable [18]. By incorporating HE, FL-based AI models can be trained across multiple mobile devices and institutions without violating privacy regulations like GDPR, HIPAA, and PCI DSS. Additionally, since encrypted model updates remain inaccessible even to the FL aggregator, HE significantly reduces the risk of insider threats, ensuring complete trust in AI model training workflows [90].

Despite its security benefits, homomorphic encryption presents significant computational challenges, particularly in real-time mobile AI applications [77]. Fully Homomorphic Encryption (FHE), which allows unrestricted encrypted computations, is extremely resource-intensive, requiring high processing power and memory bandwidth that mobile devices often lack. Even optimized variants, such as Partially Homomorphic Encryption (PHE) and Somewhat Homomorphic Encryption (SHE), introduce latency and power consumption issues, making HE impractical for low-latency AI services like real-time fraud detection or instant voice recognition [75].To address these limitations, researchers are developing hardware-accelerated HE solutions and hybrid cryptographic techniques that combine HE with lightweight encryption mechanisms to balance security and efficiency in mobile federated learning [6,95].

A major use case of homomorphic encryption in FL is encrypted AI-driven fraud detection in mobile banking [36]. Banking and financial institutions require privacy-preserving fraud detection models that can analyze transaction patterns across multiple users without exposing sensitive financial data [61]. By integrating HE into FL-based fraud detection systems, mobile banking applications can collaboratively train AI models to detect suspicious transactions, ensuring that individual financial records remain fully encrypted throughout the process. This approach enhances anti-money laundering (AML) initiatives, cross-bank fraud prevention, and secure credit scoring, making HE a critical enabler of privacy-focused financial AI ecosystems [41].

3.4. Comparative Analysis of FL Security Techniques

Table 1 Comparative Analysis of FL Security Techniques

Security Technique	Data Privacy	Computational Efficiency	Regulatory Compliance	Best Use Cases
Differential Privacy	High	High	Strong (GDPR, CCPA)	Mobile health AI, AI assistants
Secure Aggregation	Very High	Moderate	Strong (HIPAA, PSD2)	Financial transactions, IoT mobile apps
Homomorphic Encryption	Very High	Low	Strong (FIPS, ISO)	Encrypted mobile banking AI, cybersecurity models

4. Challenges in Implementing Federated Learning in Mobile Applications

4.1. Computational & Energy Constraints

One of the most significant challenges in deploying federated learning (FL) in mobile applications is the computational and energy constraints of mobile devices [47]. Unlike centralized machine learning, where AI models are trained on high-performance cloud servers, FL requires each mobile device to train AI models using its own processing power before sending encrypted updates to the central server [1]. Since smartphones and IoT devices have limited CPU, memory, and battery capacity, running complex deep learning models can lead to high energy consumption, increased latency, and device overheating. This is particularly problematic for applications that require continuous learning, such as personalized voice assistants, predictive keyboards, and real-time fraud detection, where excessive computation can drain the battery and degrade device performance [68].

To overcome these constraints, researchers and mobile AI developers are exploring lightweight AI models optimized for federated learning [77]. Techniques such as model quantization, knowledge distillation, and pruning allow AI models to be compressed and optimized for mobile hardware, reducing memory and computation demands without sacrificing accuracy. Additionally, hardware-accelerated AI chips, such as Google's Edge TPU and Apple's Neural Engine, are being integrated into mobile devices to enable efficient on-device learning [57]. However, implementing these optimizations across diverse mobile ecosystems remains a challenge, as FL must be compatible with various device architectures, operating systems, and network conditions, making large-scale deployment difficult [88].

Another key consideration is balancing energy efficiency with model performance in mobile FL applications [76]. Since federated learning requires frequent local model updates and communication with central aggregators, minimizing the frequency of updates, optimizing training schedules, and leveraging idle processing power can help reduce energy consumption [1,96]. Additionally, asynchronous FL techniques, where model updates are performed at different time intervals based on device availability and power levels, can further enhance efficiency. By developing energy-aware FL frameworks that adapt to real-time mobile constraints, researchers can make federated learning more practical for privacy-preserving AI applications, ensuring that mobile devices can support secure, decentralized model training without excessive resource depletion [34].

4.2. Security Threats in Federated Learning

Despite its privacy advantages, federated learning (FL) is vulnerable to security threats, particularly model inversion attacks, where adversaries attempt to reconstruct private user data from shared model updates [2]. Since FL does not transmit raw data, attackers exploit statistical patterns in model gradients to infer sensitive information, such as keystroke behavior, facial recognition data, or health metrics. This poses a significant risk in mobile applications like personalized healthcare, financial services, and AI-driven authentication, where privacy is critical [20]. Advanced model inversion techniques can allow attackers to recover partial or even near-complete versions of the original training data, compromising user privacy even though raw data was never explicitly shared [82].

Another major security risk in FL is poisoning attacks, where adversaries inject malicious data into the FL training process to manipulate AI model behavior [51]. This can be done in two ways: data poisoning, where attackers introduce biased or incorrect data to corrupt the training dataset, and model poisoning, where compromised devices submit altered model updates to degrade model performance or introduce hidden vulnerabilities [84]. For example, in mobile fraud detection systems, an attacker could deliberately train their local model to misclassify fraudulent transactions, leading to weakened fraud detection algorithms across the entire FL network. Since FL aggregates model updates without accessing raw data, detecting and mitigating malicious contributions remains a significant challenge [44,97].To address these threats, researchers are developing defensive techniques, such as differential privacy, secure aggregation, and anomaly detection to prevent data leakage and filter out malicious updates before model aggregation[37].Byzantine-robust federated learning frameworks can help detect and isolate compromised devices, ensuring that adversarial attacks do not significantly impact global model performance. Additionally, blockchain-based FL verification is emerging as a potential solution to enhance trust and security by ensuring tamper-proof audit trails for model updates [60]. By integrating these advanced security mechanisms, federated learning can continue to provide privacy-preserving AI solutions for mobile applications without compromising data integrity and trustworthiness [62].

4.3. Regulatory & Compliance Challenges

One of the biggest challenges in deploying federated learning (FL) in mobile applications is ensuring compliance with global data protection regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States [25].These regulations impose strict requirements on how personal data is collected, processed, and shared, particularly in AI-driven applications that handle sensitive user information like health records, financial transactions, and biometric data[53].While FL is designed to enhance privacy by keeping data on users' devices, model updates can still carry metadata or statistical patterns that could be exploited to re-identify individuals if not properly secured. To ensure regulatory compliance, organizations implementing FL must integrate privacy-preserving techniques such as differential privacy, secure aggregation, and encrypted model updates to prevent the risk of indirect data leakage [67].

Another key regulatory challenge in FL is data residency compliance, particularly in cross-border mobile AI collaborations [72]. Different countries have varying data sovereignty laws, requiring user data to remain within national or regional boundaries. In traditional AI models, organizations can enforce compliance by storing and processing data within geographically controlled cloud infrastructure, but FL's decentralized nature makes data residency enforcement more complex [17]. For instance, a global AI system deployed across European and American mobile users must ensure that model updates adhere to GDPR regulations in Europe while complying with U.S. privacy laws. This fragmentation creates legal uncertainties, making it difficult for multinational mobile applications to standardize FL implementations across different jurisdictions [15].

To address these compliance challenges, organizations must adopt privacy-aware FL frameworks that include region-specific model aggregation, ensuring that mobile devices only contribute to AI training within legally compliant data zones[23].Additionally, regulatory bodies are exploring federated governance models that enforce policy-based AI training, allowing compliance rules to be embedded directly into FL workflows [74].Emerging solutions, such as blockchain-based compliance tracking and AI-driven regulatory monitoring, can further enhance transparency and accountability in federated learning applications. By integrating these mechanisms, FL can align with global privacy laws, enabling mobile AI applications to offer privacy-preserving, legally compliant, and scalable AI solutions worldwide [61].

5. Future Trends in Federated Learning for Mobile Privacy

5.1. AI-Driven Adaptive FL for Mobile AI

One of the most promising advancements in federated learning (FL) for mobile applications is the development of AI-driven adaptive FL models, which can self-optimize based on device constraints such as processing power, memory availability, and battery life [10]. Traditional FL implementations require each mobile device to train AI models locally, but this process can be resource-intensive, particularly for devices with limited computational. Adaptive FL models use lightweight AI architecture, model pruning, and selective update mechanisms to dynamically adjust training complexity based on device performance capacity [31]. This approach ensures that even low-power mobile devices can participate in FL training without excessive battery drain, making decentralized AI more scalable and efficient for a wide range of smartphones and IoT devices [56].

Beyond efficiency, adaptive FL also enables personalized AI experiences while maintaining strong privacy guarantees [21]. In standard FL, AI models are trained collectively across multiple users, but personalization is often limited, as models must generalize across diverse datasets. With self-optimizing FL models, mobile devices can train AI models that learn from individual user behaviors, preferences, and usage patterns without compromising privacy [1]. This allows applications like voice assistants, predictive keyboards, and health monitoring apps to deliver highly customized user experiences while ensuring that sensitive data never leaves the device. By integrating adaptive FL with privacy-preserving techniques like differential privacy and secure aggregation, organizations can build AI systems that continuously improve based on user feedback without sacrificing data security [21].

As federated learning continues to evolve, the combination of AI-driven adaptive FL and privacy-enhancing technologies will drive the next generation of secure, efficient, and personalized mobile AI applications [36]. Future advancements will focus on on-device model compression, energy-efficient AI training, and decentralized AI governance to further optimize FL for large-scale mobile deployments. As AI personalization becomes a key differentiator in mobile applications, adaptive FL will play a crucial role in enabling smarter, privacy-first user experiences, paving the way for more intelligent, responsive, and secure mobile AI ecosystems [5].

5.2. Blockchain-Integrated FL for Mobile Security

As federated learning (FL) adoption in mobile applications grows, integrating blockchain technology is emerging as a powerful approach to enhance security, transparency, and trust in decentralized AI training[48].One of the key challenges in FL is ensuring the integrity and authenticity of model updates, as malicious participants can manipulate model contributions, inject poisoned updates, or attempt adversarial attacks[26].By leveraging blockchain-based decentralized model verification, FL updates can be securely recorded on an immutable ledger, allowing organizations to audit model contributions in real time. This prevents fraudulent modifications and ensures that only legitimate, high-quality model updates are included in the final AI model. Additionally, blockchain enhances trust in FL networks, particularly in cross-organizational AI collaborations where multiple entities contribute to a shared AI model[32].Beyond model verification, smart contracts on blockchain networks can be used to enforce secure FL participation and automate compliance mechanisms[40].In traditional FL setups, organizations rely on centralized aggregators to manage model updates and participant authentication, creating a potential single point of failure. With blockchain-powered smart contracts, FL processes—such as model aggregation, reward distribution, and malicious node detection—can be automated and decentralized, reducing reliance on third-party intermediaries [19]. This is particularly valuable in mobile applications that involve financial transactions, healthcare data, or biometric authentication, where trust and regulatory compliance are critical. Smart contracts can also incentivize honest participation in FL networks by rewarding genuine model contributions and penalizing malicious activity, creating a self-regulating AI ecosystem [1].

As federated learning and blockchain integration continue to evolve, decentralized AI governance frameworks will emerge, allowing mobile applications to operate in highly secure, transparent, and tamper-resistant environments [35]. Future advancements will focus on scalable blockchain consensus mechanisms, lightweight distributed ledgers, and hybrid blockchain-FL architectures to further enhance efficiency and reduce computational costs [4,98]. By combining blockchain's security and transparency with FL's privacy-preserving AI training, organizations can build next-generation mobile AI applications that are resilient against cyber threats, fraud, and unauthorized data access, ensuring both privacy and security in the decentralized AI landscape [10].

5.3. Post-Quantum Cryptography for FL-Based Mobile AI

As quantum computing advances, traditional cryptographic methods used in federated learning (FL) for mobile AI face the risk of becoming obsolete. Current encryption techniques, such as RSA and Elliptic Curve Cryptography (ECC), rely on mathematical problems that quantum algorithms could solve exponentially faster, potentially compromising the security of FL model updates and decentralized training processes [42]. To counter this threat, quantum-safe encryption techniques are being developed to ensure that FL remains secure in a post-quantum world [71].

One promising approach is the use of quantum-resistant encryption for FL model updates, where advanced cryptographic schemes protect mobile AI training data, model contributions, and aggregation processes against potential quantum-enabled attacks. By integrating post-quantum cryptographic standards into FL frameworks, mobile applications can maintain long-term data security and compliance even as quantum computing power increases [63].

A particularly effective post-quantum cryptographic technique for securing FL-based mobile AI is lattice-based cryptography [2]. Unlike traditional encryption methods that rely on factorization or discrete logarithm problems, lattice-based cryptographic algorithms leverage complex geometric structures that remain computationally hard even for quantum computers. This makes them ideal for securing mobile AI ecosystems, where federated learning updates need to be transmitted securely between millions of mobile devices without risking data leaks or adversarial inference attacks [81]. Lattice-based encryption can also be integrated into homomorphic encryption (HE) frameworks, allowing fully encrypted AI model training without exposing raw data, ensuring privacy-first AI processing for sensitive mobile applications such as biometric authentication, financial AI analytics, and mobile healthcare diagnostics [54].

As post-quantum cryptography continues to evolve, its integration into federated learning frameworks will become essential for future-proofing mobile AI security [22]. Researchers are developing lightweight quantum-resistant cryptographic algorithms that can function efficiently on low-power mobile devices, balancing computational efficiency with high levels of security. Additionally, the emergence of hybrid cryptographic models, combining classical encryption with post-quantum techniques, will enable a gradual transition toward quantum-safe FL implementations [60]. By adopting lattice-based cryptography and quantum-resistant encryption, federated learning will remain a trusted and secure AI framework, ensuring that mobile AI applications are safeguarded against both current and future cyber threats in the quantum era [59].

6. Conclusion and recommendations

Federated learning (FL) has emerged as a transformative approach to privacy-preserving AI in mobile applications, ensuring that user data remains on the device while enabling AI models to improve through decentralized training . By eliminating the need to share raw data with central servers, FL mitigates privacy risks, reduces reliance on cloud storage, and enhances compliance with data protection regulations. However, privacy and performance must be carefully balanced, which is why hybrid security models—combining FL with differential privacy, secure aggregation, and encryption techniques—have proven to be the most effective. Looking forward, blockchain-integrated FL, AI-driven optimization, and post-quantum cryptography will shape the future of secure, scalable, and resilient mobile AI ecosystems.

For researchers, the next phase of FL development should focus on hybrid security frameworks that integrate homomorphic encryption, secure aggregation, and FL to ensure end-to-end privacy and data protection. Another key area of study is AI-driven compliance automation, which can monitor FL-based models in real time to ensure they meet global regulatory standards. Additionally, optimizing lightweight cryptographic techniques tailored for resource-constrained mobile devices will be essential for making FL more efficient and scalable in large-scale deployments. For practitioners, adopting FL for mobile AI assistants, personalized recommendations, and privacy-preserving analytics is a crucial step in enhancing user trust and regulatory compliance. Implementing differential privacy in FL training will further protect user identities, ensuring that AI models learn from decentralized data without risking exposure. Moreover, leveraging blockchain-based security models for FL model verification and decentralized AI governance will help prevent data tampering, poisoning attacks, and unauthorized access, ensuring a secure, transparent, and trustworthy mobile AI ecosystem.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adako, O., Adeusi, O., & Alaba, P. Integrating AI tools for enhanced autism education: a comprehensive review. International Journal of Developmental Disabilities. 2024; 1-13.

[2] Adeusi, O. C., Adebayo, Y. O., Ayodele, P. A., Onikoyi, T. T., Adebayo, K. B., &Adenekan, I. O. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. World Journal of Advanced Research and Reviews, 22(3), 2050-2057.

[3] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., ... &Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications, 195, 346-361.

[4] Ahmed, A. A., & Alabi, O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access.

[5] Alamouti, S., Arjomandi, F., Burger, M., &Altakrouri, B. (2024). Building Blocks to Empower Cognitive Internet with Hybrid Edge Cloud. arXiv preprint arXiv:2402.00876.

[6] Alaya, B., Laouamer, L., &Msilini, N. (2020). Homomorphic encryption systems statement: Trends and challenges. Computer Science Review, 36, 100235.

[7] Alazab, M., Rm, S. P., Parimala, M., Maddikunta, P. K. R., Gadekallu, T. R., & Pham, Q. V. (2021). Federated learning for cybersecurity: Concepts, challenges, and future directions. IEEE Transactions on Industrial Informatics, 18(5), 3501-3509.

[8] Albshaier, L., Almarri, S., &Albuali, A. (2025). Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities. Electronics, 14(5), 1019.

[9] Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 8, 140699-140725.

[10] Alghamedy, F. H., El-Haggar, N., Alsumayt, A., Alfawaer, Z., Alshammari, M., Amouri, L., ... &Albassam, S. (2024). Unlocking a Promising Future: integrating Blockchain Technology and FL-IoT in the journey to 6G. IEEE Access.

[11] Ali, M., Naeem, F., Tariq, M., &Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. IEEE journal of biomedical and health informatics, 27(2), 778-789.

[12] Almutairi, S., & Barnawi, A. (2023). Federated learning vulnerabilities, threats and defenses: A systematic review and future directions. Internet of Things, 24, 100947.

[13] Alsharif, M. H., Kannadasan, R., Wei, W., Nisar, K. S., & Abdel-Aty, A. H. (2024). A contemporary survey of recent advances in federated learning: Taxonomies, applications, and challenges. Internet of Things, 101251.

[14] Amritanjali, & Gupta, R. (2025). Federated Learning for Privacy Preserving Intelligent Healthcare Application to Breast Cancer Detection. In Proceedings of the 26th International Conference on Distributed Computing and Networking (pp. 302-306).

[15] Amugongo, L. M., Kriebitz, A., Boch, A., & Lütge, C. (2023). Operationalising AI ethics through the agile software development lifecycle: a case study of AI-enabled mobile health applications. AI and Ethics, 1-18.

[16] Anitha, R., & Murugan, M. (2024). Privacy-preserving collaboration in blockchain-enabled IoT: The synergy of modified homomorphic encryption and federated learning. International Journal of Communication Systems, 37(18), e5955.

[17] Ariyibi, K. O., Bello, O. F., Ekundayo, T. F., &Ishola, O. (2024).Leveraging Artificial Intelligence for enhanced tax fraud detection in modern fiscal systems.

[18] Arora, S., & Bhatia, M. S. (2020). Fingerprint spoofing detection to improve customer security in mobile financial applications using deep learning. Arabian journal for science and engineering, 45(4), 2847-2863.

[19] Arulprakash, M., &Jebakumar, R. (2021). People-centric collective intelligence: decentralized and enhanced privacy mobile crowd sensing based on blockchain. The Journal of Supercomputing, 77(11), 12582-12608.

[20] Bala, I., Pindoo, I., Mijwil, M. M., Abotaleb, M., &Yundong, W. (2024). Ensuring security and privacy in Healthcare Systems: a Review Exploring challenges, solutions, Future trends, and the practical applications of Artificial Intelligence. Jordan Medical Journal, 58(3).

[21] Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., &Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. Information processing & management, 59(6), 103061.

[22] Bishwas, A. K., & Sen, M. (2024). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. arXiv preprint arXiv:2411.09995.

[23] Cai, Q., Cao, J., Xu, G., & Zhu, N. (2024). Distributed Recommendation Systems: Survey and Research Directions. ACM Transactions on Information Systems, 43(1), 1-38.

[24] Calvino, G., Peconi, C., Strafella, C., Trastulli, G., Megalizzi, D., Andreucci, S., ... & Giardina, E. (2024). Federated Learning: Breaking Down Barriers in Global Genomic Research. Genes, 15(12), 1650.

[25] Chalamala, S. R., Kummari, N. K., Singh, A. K., Saibewar, A., &Chalavadi, K. M. (2022). Federated learning to comply with data protection regulations. CSI Transactions on ICT, 10(1), 47-60.

[26] Chen, C., Liu, J., Tan, H., Li, X., Wang, K. I. K., Li, P., ... & Dou, D. (2025). Trustworthy federated learning: Privacy, security, and beyond. Knowledge and Information Systems, 67(3), 2321-2356.

[27] El Ouadrhiri, A., & Abdelhadi, A. (2022). Differential privacy for deep and federated learning: A survey. IEEE access, 10, 22359-22380.

[28] Emehin, O., Emeteveke, I., Adeyeye, O. J., & Akanbi, I. (2024). Securing artificial intelligence in data analytics: strategies for mitigating risks in cloud computing environments. Int Res J Modernization in Eng Tech Sci, 6, 1978-98.

[29] Fereidooni, H., Marchal, S., Miettinen, M., Mirhoseini, A., Möllering, H., Nguyen, T. D., ... & Zeitouni, S. (2021). SAFELearn: Secure aggregation for private federated learning. In 2021 IEEE Security and Privacy Workshops (SPW) (pp. 56-62). IEEE.

[30] Fouda, M. M., Fadlullah, Z. M., Ibrahem, M. I., & Kato, N. (2024). Privacy-Preserving Data-Driven Learning Models for Emerging Communication Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials.

[31] Friha, O., Ferrag, M. A., Kantarci, B., Cakmak, B., Ozgun, A., &Ghoualmi-Zine, N. (2024). Llm-based edge intelligence: A comprehensive survey on architectures, applications, security and trustworthiness. IEEE Open Journal of the Communications Society. 1(11), 21-28.

[32] GangwanI, N. (2024). Enhancing Privacy and Security in Cloud AI: An Integrated Approach Using Blockchain and Federated Learning. International Journal Of Computer Engineering And Technology, 15(5), 728-737.

[33] Habbal, A., Ali, M. K., &Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 240, 122442.

[34] Hallaji, E., Razavi-Far, R., Saif, M., Wang, B., & Yang, Q. (2024). Decentralized federated learning: A survey on security and privacy. IEEE Transactions on Big Data, 10(2), 194-213.

[35] Hammad, A., & Abu-Zaid, R. (2024). Applications of AI in Decentralized Computing Systems: Harnessing Artificial Intelligence for Enhanced Scalability, Efficiency, and Autonomous Decision-Making in Distributed Architectures. Applied Research in Artificial Intelligence and Cloud Computing, 7, 161-187.

[36] Hassan, W., & Mohamed, H. (2024). Applications of Federated Learning in AI, IoT, Healthcare, Finance, Banking, and Cross-Domain Learning. In Artificial Intelligence Using Federated Learning (pp. 175-195). CRC Press.

[37] Hathaliya, J. J., Tanwar, S., & Sharma, P. (2022). Adversarial learning techniques for security and privacy preservation: A comprehensive review. Security and Privacy, 5(3), e209.

[38] Hu, H., Salcic, Z., Sun, L., Dobbie, G., Yu, P. S., & Zhang, X. (2022). Membership inference attacks on machine learning: A survey. ACM Computing Surveys (CSUR), 54(11s), 1-37.

[39] Ikuomola, A. D. (2020). Foreign cartels and local accomplices: Socio-economic realities of criminality and deforestation in the Nigeria’s forest belts. Journal of Comparative Research in Anthropology and Sociology, 11(01), 17-33.

[40] Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys, 55(9), 1-43.

[41] Jeník, I., & Duff, S. (2020). How to build a regulatory sandbox. A Practical Guide for Policy Makers, 4-12.

[42] Kannan, E., Ravikumar, S., MJ, C. M. B., Vijay, K., Vathani, A., & Kannan, S. (2024, December). Revolutionizing Machine Learning Security: The Role of Quantum-Enhanced Federated Learning. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE

[43] Khan, M. F., &Abaoud, M. (2023). Blockchain-Integrated Security for real-time patient monitoring in the Internet of Medical Things using Federated Learning. IEEE Access, 11, 117826-117850.

[44] Khraisat, A., Alazab, A., Singh, S., Jan, T., & Jr. Gomez, A. (2024). Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. ACM Computing Surveys, 57(1), 1-38.

[45] Kishor, K. (2022). Personalized federated learning. In Federated Learning for IoT Applications (pp. 31-52). Cham: Springer International Publishing.

[46] Kuldeep, G., & Zhang, Q. (2021). Design prototype and security analysis of a lightweight joint compression and encryption scheme for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(1), 165-181.

[47] Lim, W. Y. B., Luong, N. C., Hoang, D. T., Jiao, Y., Liang, Y. C., Yang, Q., ... & Miao, C. (2020). Federated learning in mobile edge networks: A comprehensive survey. IEEE communications surveys & tutorials, 22(3), 2031-2063.

[48] Liu, J., Chen, C., Li, Y., Sun, L., Song, Y., Zhou, J., ... & Dou, D. (2024). Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. Knowledge and Information Systems, 66(8), 4377-4403.

[49] Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K. Y., & Zhao, J. (2022). Privacy-preserving aggregation in federated learning: A survey. IEEE Transactions on Big Data.

[50] Long, G., Tan, Y., Jiang, J., & Zhang, C. (2020). Federated learning for open banking. In Federated learning: privacy and incentive (pp. 240-254). Cham: Springer International Publishing.

[51] Lyu, L., Yu, H., & Yang, Q. (2020). Threats to federated learning: A survey. arXiv preprint arXiv:2003.02133.

[52] Ma, X., Chen, C., & Zhang, Y. (2024). Privacy-Preserving Federated Learning Framework for Cross-Border Biomedical Data Governance: A Value Chain Optimization Approach in CRO/CDMO Collaboration. Journal of Advanced Computing Systems, 4(12), 1-14.

[53] Mbonye, V., Moodley, M., & Nyika, F. (2024). Examining the applicability of the Protection of Personal Information Act in AI-driven environments. South African Journal of Information Management, 26(1), 1808.

[54] Mukkamala, S. S. K., Mahida, A., &Vishwanadham Mandala, M. S. (2024). Leveraging AI And Big Data For Enhanced Security In Biometric Authentication: A Comprehensive Model For Digital Payments. Migration Letters, 21(8), 574-590.

[55] Narula, M., Meena, J., & Vishwakarma, D. K. (2024). A comprehensive review on federated learning for data-sensitive application: Open issues & challenges. Engineering Applications of Artificial Intelligence, 133, 108128.

[56] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1622-1658.

[57] Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet of Things Journal, 8(16), 12806-12825.

[58] Nwanna, M., Offiong, E., Ogidan, T., Fagbohun, O., Ifaturoti, A., &Fasogbon, O. (2025). AI-Driven Personalisation: Transforming User Experience Across Mobile Applications. Journal of Artificial Intelligence, Machine Learning and Data Science.

[59] Nwoye, C. C. (2024). Next-generation protection protocols and procedures for securing critical infrastructure. International Journal of Research Publication and Reviews, 5(11), 4830-4845.

[60] Olawale, A., Ajoke, O., &Adeusi, C. (2020).Quality assessment and monitoring of networks using passive.

[61] Olowu, O., Adeleye, A. O., Omokanye, A. O., Ajayi, A. M., Adepoju, A. O., Omole, O. M., &Chianumba, E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity.

[62] Padmanaban, H. (2024). Privacy-preserving architectures for AI/ML applications: methods, balances, and illustrations. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 235-245.

[63] Papadopoulos, C., Kollias, K. F., &Fragulis, G. F. (2024). Recent Advancements in Federated Learning: State of the Art, Fundamentals, Principles, IoT Applications and Future Trends. Future Internet, 16(11), 415.

[64] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., &Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. International Journal on Soft Computing, 14(3), 01-16.

[65] Prieto, J. (2024). Case Studies in Federated Learning for Healthcare. Federated Learning and Privacy-Preserving in Healthcare AI, 91.

[66] Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., &Piccialli, F. (2024). Model aggregation techniques in federated learning: A comprehensive survey. Future Generation Computer Systems, 150, 272-293.

[67] Rahman, A., Hasan, K., Kundu, D., Islam, M. J., Debnath, T., Band, S. S., & Kumar, N. (2023). On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Computer Systems, 138, 61-88.

[68] Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 14(8), 10517-10553.

[69] Raza, A. (2023). Secure and privacy-preserving federated learning with explainable artificial intelligence for smart healthcare system. University of Kent (United Kingdom).

[70] Razi, Q., Piyush, R., Chakrabarti, A., Singh, A., Hassija, V., &Chalapathi, G. S. S. (2025). Enhancing Data Privacy: A Comprehensive Survey of Privacy-Enabling Technologies. IEEE Access.

[71] Ren, C., Yu, H., Peng, H., Tang, X., Zhao, B., Yi, L., ... & Yang, Q. (2024). Advances and Open Challenges in Federated Foundation Models. arXiv preprint arXiv:2404.15381.

[72] Rong, K., Ling, Y., Yang, T., & Huang, C. (2025). Cross-border data transfer: patterns and discrepancies. Journal of International Business Policy, 1-23.

[73] Saeed, M. M., &Alsharidah, M. (2024). Security, privacy, and robustness for trustworthy AI systems: A review. Computers and Electrical Engineering, 119, 109643.

[74] Salim, M. M., Yang, L. T., & Park, J. H. (2024). Privacy-preserving and scalable federated blockchain scheme for healthcare 4.0. Computer Networks, 247, 110472.

[75] Sanon, S. P., Ademi, I., Zentara, M., &Schotten, H. D. (2024). Applicability of fully homomorphic encryption in mobile communication. In 2024 3rd International Conference on 6G Networking (6GNet) (pp. 234-240). IEEE.

[76] Shi, D., Li, L., Chen, R., Prakash, P., Pan, M., & Fang, Y. (2022). Toward energy-efficient federated learning over 5G+ mobile devices. IEEE Wireless Communications, 29(5), 44-51.

[77] Singh, A., Satapathy, S. C., Roy, A., &Gutub, A. (2022). Ai-based mobile edge computing for iot: Applications, challenges, and future scope. Arabian Journal for Science and Engineering, 47(8), 9801-9831.

[78] Singh, R., & Gill, S. S. (2023). Edge AI: a survey. Internet of Things and Cyber-Physical Systems, 3, 71-92.

[79] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 1-18.

[80] Sumathi, D., Botta, L. C., Reddy, M. S. J., & Das, A. (2025). Federated Learning: Bridging Data Privacy and AI Advancements. Model Optimization Methods for Efficient and Edge AI: Federated Learning Architectures, Frameworks and Applications, 157-168.

[81] Tuncel, Y. K., &Öztoprak, K. (2025). SAFE-CAST: secure AI-federated enumeration for clustering-based automated surveillance and trust in machine-to-machine communication. PeerJ Computer Science, 11, e2551.

[82] Veeraragavan, N. R., Boudko, S., & Nygård, J. F. (2024). A Multiparty Homomorphic Encryption Approach to Confidential Federated Kaplan Meier Survival Analysis. arXiv preprint arXiv:2412.20495.

[83] Vyas, A., Lin, P. C., Hwang, R. H., & Tripathi, M. (2024). Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey. IEEE Access.

[84] Wang, Z., Ma, J., Wang, X., Hu, J., Qin, Z., & Ren, K. (2022). Threats to training: A survey of poisoning attacks and defenses on machine learning systems. ACM Computing Surveys, 55(7), 1-36.

[85] Williamson, S. M., &Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. Applied Sciences, 14(2), 675.

[86] Xie, Q., Jiang, S., Jiang, L., Huang, Y., Zhao, Z., Khan, S., ... & Wu, K. (2024). Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey. IEEE Internet of Things Journal, 11(14), 24569-24580.

[87] Zhang, J., Zhu, H., Wang, F., Zhao, J., Xu, Q., & Li, H. (2022). Security and privacy threats to federated learning: Issues, methods, and challenges. Security and Communication Networks, 2022(1), 2886795.

[88] Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., &Avestimehr, A. S. (2022). Federated learning for the internet of things: Applications, challenges, and opportunities. IEEE Internet of Things Magazine, 5(1), 24-29.

[89] Zhao, Y., & Chen, J. (2022). A survey on differential privacy for unstructured data content. ACM Computing Surveys (CSUR), 54(10s), 1-28.

[90] Zheng, Y., Chang, C. H., Huang, S. H., Chen, P. Y., & Picek, S. (2024). An Overview of Trustworthy AI: Advances in IP Protection, Privacy-preserving Federated Learning, Security Verification, and GAI Safety Alignment. IEEE Journal on Emerging and Selected Topics in Circuits and Systems.2(12), 35-40.

[91] Zhu, T., Ye, D., Wang, W., Zhou, W., & Philip, S. Y. (2020). More than privacy: Applying differential privacy in key areas of artificial intelligence. IEEE Transactions on Knowledge and Data Engineering, 34(6), 2824-2843.

[92] Adeusi, O. C., Adebayo, Y. O., Ayodele, P. A., Onikoyi, T. T., Adebayo, K. B., &Adenekan, I. O. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. World Journal of Advanced Research and Reviews, 22(3), 2050-2057.

[93] David, A. A., & Edoise, A. (2025). Cloud computing and Machine Learning for Scalable Predictive Analytics and Automation: A Framework for Solving Real-world Problem.

[94] Onah, L. K., Temitope, S. A. (2024). Examining the integration of Artificial intelligence in automated building construction and design optimization.

[95] Temitope, S. A., & Onah, l. k. (2024). Exploring machine learning algorithms for automating complex processes in building landscape architecture.

[96] Onah, L. K., Temitope, S. A. (2024). Examining the integration of Artificial intelligence in automated building construction and design optimization.

[97] Ariyibi, K. O., Bello, O. F., Ekundayo, T. F., &Ishola, O. (2024). Leveraging Artificial Intelligence for enhanced tax fraud detection in modern fiscal systems.

[98] Temitope, S. A., Onah, L. K. & Rajat, GInnovative architectural design practices enabled by AI powered parametric and computational approaches. 2024.