Communication in Physical Sciences 2023, 9(4): 870-887

A Comprehensive Review of Edge Computing Approaches for Secure and Efficient Data Processing in IoT Networks

Michael Oladipo Akinsanya, Aminath Bolaji Bello* and Oluwafemi Clement Adeusi.
Received: 03 May 2023/Accepted: 09 September 2023/Published: 19 September 2023

Abstract: *The exponential growth of IoT networks brings the related concerns of data security, privacy, and regulatory compliance to the fore, especially when threats to traditional cloud-based processing models include latency, cyberattacks, and unauthorized access to the data. Edge computing emerged as a decentralized solution that brings data processing closer to IoT devices to reduce single points of failure while enhancing real-time threat detection. In this paper, we examine some of the most important security technologies for edge-based IoT environments, such as Trusted Execution Environments (TEEs) and their use in conjunction with homomorphic encryption and federated learning, analyzing their strengths and weaknesses. It highlights scalability challenges, security vulnerabilities, and regulatory compliance issues within edge computing. Other emerging trends like blockchain-integrated edge AI, post-quantum cryptography, and self-learning cybersecurity models will enable the next generation of secure, privacy-preserving IoT ecosystems. By adopting hybrid security frameworks and adaptive AI-driven security mechanisms, firms can guarantee a robust, scalable, and compliant edge computing solution for IoT networks.*

Keywords: *Edge Computing, IoT Security, Federated Learning, Homomorphic Encryption and Decentralized AI*

Michael Oladipo Akinsanya*
School of Computing, Wichita State University, Kansas, USA
Email: oladipoakinsanya@gmail.com

Aminath Bolaji Bello*
Department of Mathematical Sciences, Faculty of Science, Adekunle Ajasin University, Akungba Akoko, Ondo State, Nigeria
Email: bellobolaji07@gmail.com

Oluwafemi Clement Adeusi
Department of Computer Science Network and Security, Staffordshire University, UK
Email: ocadeusi@gmail.com

1.0 Introduction

Artificial Intelligence (AI) and Machine Learning (ML) have begun transforming various interdisciplinary fields by providing dependable solutions for data analysis, real-time decision-making, and autonomous navigation with an environmental solutions to the problems and to Secure and Efficient Data Processing in IoT Networks (Abolade, 2023; Ademilua, 2021; Ufomba & Ndibe, 2023; Ufomba & Ndibe, 2023). Ademilua & Areghan, 2022).

The rise in the Internet of Things (IoT) networks has changed industries like smart cities, healthcare, industrial automation, and autonomous vehicles. Millions of IoT devices are generating trillions of data points in real-time, mostly processed in centralized environment systems such as cloud (Humayun, 2020). This introduces a lot of security risks to the data because, with the transmission of sensitive data to the cloud, such data becomes an easy target for cyber-attacks and unauthorized access of different users, which can even lead to losing data (Chataut et al., 2023). Centralized systems cannot cope with such amounts of data because the volumes are becoming bigger every day with the IoT

adoption trend; hence, the applications tend towards being real-time but have high latencies and inefficiencies.

Cloud-based IoT processing also poses challenges in keeping up with national security, that is, compliance with laws such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the IoTCybersecurity Improvement Act, which require organizations to maintain secure locations for storing and processing information as well as their transfer (Umair et al., 2021).

Kong et al. (2022) established that it is edge computing that has proved to be a revolutionary option in addressing security challenges within IoT by moving data processing nearer the source, on IoT devices, gateways, or edge servers-rather than depending on very remote cloud infrastructure. This decentralized processing would reduce single points of failure so that if the cloud server is compromised, sensitive IoT data is still secure at the network edge. Edge computing will improve the IoT detection and response against threats because real-time decision-making is performed at the device level, thus preventing cyberattacks from happening before they escalate (Nain et al., 2022). Since local processing takes place, less sensitive data is transferred over the networks, and therefore less exposed to hacking attempts, data interception, and unauthorized surveillance.

The elimination of cloud-latency issues, which are critical in time-sensitive applications such as autonomous driving, industrial automation, and remote healthcare monitoring, is another key benefit of edge computing for IoT security (Kong et al., 2022). Any amount of hold-up in data transmission or processing in these environments can result in safety risks, operational failures, or inappropriate real-time analysis. Edge computing ensures processing takes place in real time, allowing instantaneous real-time anomaly detection, cybersecurity monitoring, and AI-enabled decision-making (Ogu *et. al.,* 2021). This is a direct boost to sectors of critical infrastructure whose security breaches in IoT could result in catastrophic infrastructure failures, financial losses, or possible life-threatening conditions.

In addition to better security and performance, edge computing improves privacy and compliance with regulations because IoT devices can process data locally and avoid transferring data to cloud data centers (Losavio, 2020). For instance, stricter laws like GDPR and CCPA prohibit cross-border data transfers along with centralized data collection, thus necessitating the need for strong data protection mechanisms by organizations. Keeping sensitive data in local networks allows companies to comply with rules regarding storing private information without compromising users' trust and data integrity. Also, secured edge AI models combining machine learning and encryption techniques for analysis further strengthen privacy-preserving IoT analytics (Mathew, 2022).

George, *et. al.,* (2023) contend that edge computing's rising relevance in IoT security is ending because it has become widely adopted across industries. Global edge computing is estimated to thrive from $53 billion in 2023 to $111 billion by 2028, indicating a strong demand for decentralized processing solutions. According to Alotaibi (2023), 90% of enterprises with IoT security strategies have adopted or plan to adopt edge computing in their privacy and threat mitigation efforts. Top companies in technology have ventured into the realm of secure edge AI frameworks; for instance, Google has Edge TPU, Amazon has AWS Greengrass, and Microsoft has Azure IoT Edge (Koul, *et. al.*, 2019).

As IoT networks continue to grow, edge computing will be critical in ensuring data processing with the secure, efficient, and regulatory compliance needed. This paper examines some of the key security technologies that enable edge-based IoT protection, such as

secure enclaves, homomorphic encryption, and federated learning (Parveen & Basit, 2023). Furthermore, the work discusses scaling challenges that affect edge security: performance trade-offs, regulatory complexities, and newer cybersecurity threats (Achuama, 2023). Finally, the study considers future trends in edge-based IoT security, such as blockchain integration, quantum-safe cryptography, and AI-driven automated threat detection. Privacy-preserving edge computing strategies will provide organizations with a more secure and resilient IoT ecosystem.

2.0 Security Technologies for Edge-Based IoT Data Processing

2.1 Secure Enclaves & Trusted Execution Environments (TEEs)

Secure Enclaves and Trusted Execution Environments (TEEs) offer a dedicated protection mechanism against threat agents for data processing going on at the edge (Shepherd, 2019). TEEs represent a secure area within a processor that protects data and computation, insulating them from compromise of any nature, (Lijoka, 2021; Edoh, *et. al.*, 2023). Another way that TEEs differ from standard encryption models is that while encryption methods look at protecting data in transit or at rest, TEEs protect data during computation, assuring that sensitive IoT data is processed free of exposure to unauthorized entities. For edge IoT computing, TEEs give rise to confidential computing, which permits IoT devices to execute code securely in an enclave, putting a lid on malicious software and untrusted applications as well as curtailing attackers from accessing sensitive information (Kurnikov, 2021).

One of the prominent advantages of the TEEs is the prevention of insider attacks and guaranteeing hardware-based security. Dave (2021) said since IoT devices are deployed in places that cannot be trusted, they are commonly under the likelihood of being tampered with, unauthorized, or attacked by malware. TEEs cater to solving these potential risks by limiting sensitive computation to well-defined trusted bounds, ensuring that sensitive data can only be properly processed by authorized applications (Choi & Butler, 2019). Furthermore, remote attestation in TEEs is secure, enabling the organization to verify IoT device integrity prior to permitting network access. The ability to have such assurance makes TEEs valuable in sectors where data confidentiality and trustworthiness matter, such as in financial transactions, smart grids, or autonomous vehicles (Lee et al., 2023).

The above notwithstanding, the major limitations for secure enclaves and TEEs relate to limited computational resources and side-channel attack vulnerability. With the TEE's operations occurring in a constrained hardware environment, it has limitations in processing power, which can be detrimental to performance in highly complex AI-driven IoT applications (Olawale et al., 2020). These side-channel attacks are obviously outside of, not able to target any set protection, whereby the methods of trace by means possibility are power consumption, through electromagnetic signals, and/or through variations in device execution time. The side-channel attacks have yielded a successful target so far, such as Cache attacks and Speculative Execution attacks against Intel SGX and ARM TrustZone. Thus, requiring a bolstering through continuous security updates along with efficient countermeasures (Wang et al., 2023).

TEEs majorly apply to IoT security in an edge-based context in medical IoT and industrial control systems and TEE protects healthcare-related electronic health records (EHR), remote patient monitoring data, and AI diagnostics from unauthorized access. Secure enclaves help ensure that only authorized medical personnel or applications are permitted to act on sensitive patient data, which helps mitigate risks from data breaches and regulatory violations (for instance, HIPAA and GDPR)

(Liu et al., 2023). In the context of industrial automation, TEEs would protect real-time control systems, manufacturing robots, and critical infrastructure sensors from cyberattacks and sabotage attempts. With TEEs, smart factories and energy grids can ensure that no external code injection would halt or compromise the operations (Kumar et al., 2023).

2.2 Homomorphic Encryption for Encrypted Edge Processing

Munjal & Bhatia (2023) explain that a homomorphic encryption (HE) technique is a cryptographic mechanism allowing the execution of computations on encrypted data without decryption, thus guaranteeing that sensitive IoT data remains confidential during processing. HE is different from typical encryption, in which the data must be decrypted for processing, thereby introducing security breaches, in that IoT devices and edge computing systems operate on mathematical computations on data directly in encrypted form (Pachghare, 2019). This ability is particularly important for privacy-preserving edge AI scenarios, which involve the processing of vast amounts of personal, financial, and operational data by IoT networks, the confidentiality of which must be preserved, regardless of how compromised these devices are or how physical access is granted to the attackers (Le & Shetty, 2022). HE can assist organizations to perform secure machine-learning models and analytics on IoT-generated data and automation without exposing raw data (Olawale et al., 2020).

End-to-end data privacy security is largely guaranteed against any unscrupulous environment, and this is a hallmark of homomorphic encryption security. The HE algorithm will guarantee that even if an edge device is hacked into, an attacker will not be able to decrypt any encrypted data, even though most of the time, IoT devices will be operating in a distributed, unsecured environment (Ali et al., 2023). Therefore, HE can be applicable for sensitive solutions such as financial transaction security, healthcare data analysis, and military-grade communication systems about the IoT. Additionally, HE promotes regulatory compliance for organizations by enabling them to process data pertaining to privacy laws, such as GDPR, HIPAA, and PCI DSS, yet without divulging sensitive information to any third parties.

However, from the security perspective, the biggest challenge with HE is its strong performance limitations: computation overhead. Fully Homomorphic Encryption (FHE) invokes the highest computational resources, impacting any working real-time application in IOT-such as autonomous driving, industrial automation, or smart surveillance (Liu & Han, 2019; Nguyen, *et. al.*, 2022) further FHE is the most resource-hungry computation. Up next in high computational requirements, causing high latency and energy consumption, remain the more efficient variants of HE-partially Homomorphic Encryption (PHE) and Somewhat Homomorphic Encryption (SHE) (Brakerski et al., 2023). In such constraint scenarios, HE implementation in low-power edge devices is nearly impossible, requiring optimized hardware accelerators, hybrid cryptographic methods, and specific AI models that boost efficiency.

Secure smart grid energy analytic and financial IoT transactions secure smart grids that depend on IoT sensors to monitor energy consumption using HE to process encrypted meter readings without revealing personal usage information. Thus, blocking cyberattacks on energy infrastructure and ensuring grid security and privacy (Zhang et al., 2023). Similarly, in financial IoT applications such as contactless payments, HE promotes secure edge analytics and fraud detection while maintaining customer data secrecy on blockchain-based transaction systems and decentralized finance

(DeFi) systems. Integrating HE into IoT financial systems allows organizations to prevent data leakage, secure transaction mechanisms, and comply with mandated financial regulations, paving the way for privacy-first IoT finance solutions.

2.2 Federated Learning for Privacy-Preserving Edge AI

The federated learning is a decentralized ML approach where the IoT devices may train the models locally instead of sharing raw data, thereby optimizing privacy and security in any edge computing world (Adelusi, *et. al.*, 2023). Classical ML models sink in because they depend on centralized cloud servers and large-scale transfers of data from IoT devices into the big cloud. This produces risks of cyberattacks, potential data breaches, and violations of regulations. FL diminishes the risks since every IoT device can train its local model and share updates to the aggregated one with the central coordinator as oppose to sharing the original data. The decentralized functioning of FL becomes very important for any privacy-sensitive IoT apps such as healthcare wearables, industrial IoT (IIoT), and networks of autonomous vehicles in which data privacy and compliance with regulations are of utmost importance (Aouedi, *et. al.*, 2022).

The strong key with FL in IoT is that it can strengthen data security while satisfying regulations, including GDPR, HIPAA, and CCPA. With the FL approach, the raw data never leaves its local device, thus reducing the risk of data interception and unauthorized access; hence, confidentiality is warranted in distributed IoT ecosystems (Chalamala et al., 2022). Furthermore, it promotes healthy cross-institutional collaborations without exposing sensitive data, thereby allowing multiple IoT networks to train shared AI models complying with regional data privacy laws. Such features make FL especially enterprising in cybersecurity threat detection, where real-time insights drawn from several IoT nodes can enhance anomaly detection and attack prevention across the network (Reddy, 2021; Nguyen, *et. al.*, 2022).

However, FL suffers from scalability issues and insecure communications, especially with respect to high overhead for communication and susceptibility to attacks such as model poisoning, wherein malicious actors. They are posing themselves as model participants to corrupt an FL model. Since FL updates and aggregates model parameters on an ongoing basis from distributed IoT devices and central aggregators, this could produce some latency and put some stress on the bandwidth, especially for larger IoT deployments (Bouacida & Mohapatra, 2021). Model poisoning attacks are those whereby adversaries masquerade as legitimate nodes and submit updates that undermine the learning processes. Their target is to bias an FL system in such a way that it serves their nefarious aims. Such discrimination may exploit these weaknesses and bias fraud detection systems, corrupt cybersecurity threat models, or dilute anomaly detection in critical infrastructure (Ode-Martins, 2021). Therefore, secure aggregation techniques, differential privacy, and robust anomaly detection algorithms for filtering out corrupted updates must be put in place in every implementation of FL (Uzozie *et. al.*, 2023).

A key use case of federated learning in IoT covers, among others, anomaly detection in connected vehicles and cybersecurity threat prediction. In autonomous vehicle networks, FL allows smart cars to work together so as to improve AI models in the areas of traffic pattern recognition, collision avoidance, and predictive maintenance, all while ensuring the privacy of individual vehicle data (Yang et al., 2023). Likewise, in IoT-driven cybersecurity, FL enables edge devices to detect malware, phishing attempts, and network anomalies in real time based on distributed threat intelligence from multiple IoT sources (Li et al., 2023). This integration means that an FL approach could allow organizations to build

resilient privacy-preserving AI-driven defences for the IoT realm of tomorrow.

3.0 Challenges in Adopting Secure Edge Computing for IoT

3.1 Scalability & Performance Trade-offs

Egwuche *et. al.,* (2021) explained that one major challenge in providing secure edge computing for IoT is further resource constraints of edge devices, which restrict the performance of AI-driven threat detection and encryption techniques. Unlike cloud-based data centers, which provide high computing power and storage capability, IoT edge devices mostly run on low-power processors that have limited memory and energy. Latency issues caused by slower response times and power consumption are common among these constrained devices when running advanced AI models, encryption algorithms, and real-time security analytics (Singh et al., 2022).

Table 1: Security Technologies, Their Properties, and Use Cases

Security Technology	Data Privacy	Computational Efficiency	Regulatory Compliance	Best Use Cases
Secure Enclaves (TEEs)	High	Moderate	Strong (FIPS, GDPR)	Medical IoT, smart factories
Homomorphic Encryption	Very High	Low	Strong (HIPAA, PCI DSS)	Financial IoT, edge-based healthcare AI
Federated Learning	High	Moderate	Strong (CCPA, GDPR)	Cybersecurity, fraud detection

This creates a trade-off between security and performance, as more robust encryption techniques-such as homomorphic encryption and secure enclaves (TEEs)-require significant processing power, which many IoT devices lack. Consequently, organizations should seek mechanisms that harmonize security with computational effectiveness in edge computing environments (Ofili, Obasuyi & Akano, 2023). Optimization on energy-efficient machine learning (ML) models runs effectively on resource-constrained IoT devices, which is an important area of research and development against the backdrop of these limitations. These techniques include model quantization, edge AI accelerators, and lightweight encryption algorithms, which can be explored to enhance real-time threat detection and anomaly identification without rendering device resources overburdened (Smith et al., 2023). Concerning data training and sharing by various edge devices, federated learning (FL) provides such an opportunity, as locally trained ML models do not have to send raw data to the cloud, thereby eliminating network congestion and delays due to processing. Conversely, even FL cannot eliminate the communication overhead since model updates need to be synchronized across multiple edge nodes. To improve operational efficiency, hardware accelerators such as Google Edge TPU and NVIDIA Jetson have been integrated into organizations, such as those specifically engineered for AI inference at the edge (Sun & Kist, 2021).

Challenges also exist in terms of scalability despite emerging trends. Scalability will become an issue in large-scale IoT networks, in which several thousands or even millions of devices are interconnected. The bigger the edge infrastructure becomes, the more complicated security data processing, encryption, and citation of workloads based on artificial intelligence become over the distributed nodes (Brown et al., 2023). In addition, some applications might necessitate further edge-to-

cloud coordination for added data synchronization and security management burdens. To address these challenges, hybrid edge-cloud models for such workloads, automated hiring strategies for resources, and adaptive AI models matching intelligently compute power in accordance with workload demands will be vital (Taylor et al., 2023). Once such performance trade-offs have been addressed, secure edge computing can boost privacy, scalability, and real-time security for IoT networks.

3.2 Security Threats in Edge-Based IoT

The Trusted Execution Environments (TEEs), traditionally catering to the secure enclave for sensitive computations, are now vulnerable to attacks such as side-channel analysis. Any side channels, such as those involving power consumption analysis, electromagnetic radiation leakage, or cache-based timing variations, could allow an attacker to infer confidential information (Johnsson & Nordling, 2023). This is attested by researchers, who demonstrated that the very frequently used TEE tech, Intel SGX, could fall prey to speculative execution attacks like Foreshadow. Under IoT scenario contexts, devices are operating in trusted or untrusted locations, subjecting them to threats if malicious parties extract encryption keys, modify firmware, or gain unauthorized access to device operations (Valadares et al., 2021). Mitigation would call for attacking these threats through continuous firmware updates utilizing better cryptographic shielding and AI-enabled attack detection, wherein it would report abnormal patterns in hardware behaviour.

Edge-to-cloud communication, in another respect, is vulnerable to MITM attacks. Since IoT devices transmit data using various wireless protocols (Wi-Fi, 5G, LoRaWAN, Zigbee, etc.), these communications can be intercepted, manipulated, or redirected by attackers, leading to data leakage and device hijacking or injection of malicious commands (Garcia et al., 2023). Edge computing subsystems are designed to minimize dependence on the cloud by carrying out processing locally; however, some tasks, such as remote device management, firmware updates, or heavy AI model training, may depend on the cloud. Should the end-to-end communication performed by the edge devices rely on an encryption scheme such as TLS 1.3 or quantum-safe cryptographic protocols together with strong authentication mechanisms, an attacker could pose as a legitimate service, steal some credentials, or inject malicious software into the system (Patel et al., 2023). Organizations must, therefore, adopt a zero-trust security architecture, decentralized identity frameworks (blockchain-based authentication), and IDSs that monitor real-time anomalous behaviour in the network to mitigate the above points.

Adversarial AI attacks on federated learning (FL) models represent another blossoming risk for secure edge-based IoT environments. FL allows machine learning models to be trained across distributed IoT devices without sharing raw data, thereby ensuring privacy (Ferrag et al., 2023). Yet, malicious IoT nodes in FL training can inject poisoned data that leads the AI models into incorrect predictions for applications like autonomous vehicle navigation, healthcare diagnostics, or cybersecurity threat detection (Nguyen et al., 2021). Attacks may also target model inversion, whereby attackers infer sensitive training data from model updates, thus breaking privacy. To mitigate these threats, organizations should leverage differential privacy mechanisms, Byzantine fault tolerance, and secure aggregation protocols to filter out false model updates and uphold federated learning integrity in IoT networks (Olawale et al., 2020).

4.0 Regulatory & Compliance Issues

Furthermore, one of the crucial arguments in secure edge computing for IoT is ensuring that the decentralized data is processed in

compliance with data protection regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Hartmann, *et. al.,* 2022). In traditional cloud-based models, centralized monitoring and enforcement of data privacy rules are facilitated, but under edge computing, data homeowners process their data locally through IoT devices, gateways, or edge servers, making it hard to ensure uniform security policies through distributed nodes (Politou et al., 2022). Regulations concerning GDPR state strict rules of personal data control, be it data residency, the right to be forgotten, or explicit user consent. In most cases, this might be stringent yet difficult to achieve in a decentralized edge environment. The same applies to healthcare IoT applications in which HIPAA specifies that patient data must be securely stored, processed, and transmitted; however, edge-based medical devices and wearables cannot be integrated because they usually do not have standard encryption or secure access controls, which increases the chance of noncompliance and legal penalties (Gerlach et al., 2022).

The above conditions are put forward by another major factor to define edge-based IoT security concerns: the problem of identity authentication and secure sharing of data. For example, cloud-based authentication relies solely on centralized user verification for any authentication. Edge IoT devices, on the other hand, require lightweight, decentralized authentication mechanisms able to work autonomously from the built-in interfaces of their systems and with no compromise on their safety (Anderson et al., 2023). Traditional password authentication is not sufficient for edge networks because an IoT device only has autonomous functional capabilities for the authentication process and there are no interfaces for user interaction. In addition to all of that, data-sharing agreements between heterogeneous IoT ecosystems-such as connected vehicles, industrial automation, and smart healthcare networks, raise issues of trust given who can access sensitive information and under what conditions. Implementation of blockchain-based decentralized identity (DID) frameworks along with zero-trust security models could enforce safeguard authentication over edge IoT networks, but such solutions require collaboration in terms of standardization and scalability by industry participants (Taylor et al., 2023).

A critical issue that hampers the momentum in the adoption of secure edge computing is the lack of standardization in security protocols across differing IoT networks. Different custom-built security implementations are generated by various industry and manufacturer-specific, leading to fragmented and thus difficult-to-integrate, audit, and regulate security structures (Brown et al., 2023). Universal security frameworks are lacking, and this has prevented organizations from keeping data encryption, firmware updates, and interoperability of the edge computing environment secure and consistent. Initiatives like ISO/IEC 27001 for IoT security, the NIST Cybersecurity Framework, and the Edge Computing Consortium (ECC) are working to define standardized best practices, but these efforts face challenges in widespread adoption. To achieve scalable, regulatory-compliant edge computing, IoT stakeholders must collaborate on unified frontiers-security standards, automated compliance monitoring, and privacy-enhancing technologies (PETs) aligned with developing global regulations (Smith et al., 2023).

5.0 Future Trends in Secure Edge Computing for IoT

5. 1 : Blockchain-Integrated Edge AI for IoT Security

In the opinion of Aramide (2023), the adoption of blockchain and AI-driven security mechanisms for decentralized identity verification is the most promising advancement in secure edge computing for IoT. By making central identity providers, the general IoT

authentication systems are exposed to being hacked, credentials stolen, or attacked from the inside. With Blockchain, Decentralized Identity (DID) frameworks, IoT devices can authenticate without a central authority (Badidi, 2022). Upon registering IoT devices, a unique cryptographic identity is assigned to each device, which is tamper-proofly recorded in the blockchain ledger and serves as a think pyramid of trust, transparency, and resistance to identity-spoofing. This makes the application of this method more ideal in critical IoT environments such as smart cities, autonomous vehicles, and industrial automation environments, since verifying whether a device is legitimate or not is an essential safeguard against unauthorized access and other cyber threats (Chukwudebe, *et. al.*, 2021).

Another area of ground-breaking transformation is where security policies based on smart contracts may be used to control IoT access control and automated enforcement of cybersecurity measures. Unlike the traditional role-based or rule-based authentication methods, smart contracts could provide self-executing decentralized mechanisms through which only authorized devices, users, or applications could use sensitive IoT data (Garcia et al., 2023). For health-based connected environments, for instance, smart contracts can as required open and close access to patient records based on regulatory compliance and patient consent, thus ensuring minimal unauthorized data exposure. Similarly, in industrial IoT networks, smart contracts may put in place automatically enforced security rules that could prevent malicious devices from accessing essential infrastructure (Patel et al., 2023). Integrating blockchain with Edge AI, therefore, enables organizations to develop self-governing IoT ecosystems that exhibit maximum resilience against cyber threats, besides being transparent, auditable and compliant with regulations.

5.2 Quantum-Safe Cryptography for Edge-Based IoT Security

Chawla and Mehra (2023) argue that with the advancement of quantum computing, the traditional cryptographic techniques used in the security domain of IoT could become irrelevant, making quantum-resistant encryption imperative for protecting edge-based IoT networks. Although current encryption approaches like RSA and ECC rely on those very mathematical problems that could be broken by quantum computers through algorithms such as Shor's (Erondu, *et. al.,* 2022), lattice-based cryptography is being researched for quantum-safe encryption against classical and quantum attacks. By implementing lattice-based encryption within edge computing frameworks, IoT devices can continue to safeguard sensitive communications, provide user authentication, or secure decentralized data processing in a post-quantum world (Ukwuoma, *et. al.,* 2022). This holds particular importance for autonomous vehicles, industrial control systems, and military IoT networks, where the long-term availability of data security is of utmost importance.

Another important advancement impacting quantum-safe IoT security is the post-quantum secure machine-learning models for real-time cybersecurity threat detection at the edge. Moreover, if quantum computing advances to enable more challenging adversarial attacks or faster model inversion, traditional AI-driven anomaly detection and intrusion prevention systems could be compromised (Hassan, *et. al.,* 2021). By designing quantum-resistant AI models that leverage lattice-based signatures and hash-based cryptography, edge devices can maintain robust threat detection and response capabilities against both conventional and quantum-enabled cyber threats (Taylor et al., 2023). Adopting post-quantum cryptographic standards in edge-based IoT security architectures will, therefore, be paramount to guaranteeing long-term cybersecurity

resilience, regulatory compliance, and trust in next-generation IoT ecosystems.

5.1 AI-Driven Automated Security at the Edge

AI making security at the edge reactive and auto-piloting will be the last bastion, since threats towards IoT networks are becoming very advanced (Yaseen, 2023). The conventional security solutions are based on static rules and are unable to keep pace with evolving attack patterns. In contrast, self-learning AI models can independently analyze real-time threat intelligence for detecting anomalies and acting against cyberattacks (Tanikonda et al., 2022). These models use ML and deep learning techniques to identify malware, intrusion attempts, and zero-day vulnerabilities at the edge while minimizing human intervention. Through the deployment of AI-powered cybersecurity frameworks in edge computing, IoT devices can carry out localized threat mitigation and reduce dependency on cloud security mechanisms, which unwarrantedly increase latency and bandwidth constraints (Butun, *et. al.,* 2019).

To further enhance edge-based IoT security, researchers are working on adaptive federated learning techniques, which give AI models access to learn from many IoT devices without exchanging raw data. In contrast with centralized ML training, federated learning (FL) would permit decentralized sharing of threat intelligence to aid devices in improving AI security models cooperatively while preserving the privacy of their data (Yaseen, 2023). Asynchronous FL training continuously advances IoT security by updating ML models to identify new attack vectors, while also ensuring compliance with regulations (e.g., GDPR, HIPAA) (Olowononi, Rawat & Liu, 2020). This is especially useful in critical industrial sectors such as healthcare, autonomous vehicles, and industrial automation, under which the response to security attacks must be immediate. The synergy of self-learning AI models and federated learning may evolve edge computing into a proactive and intelligent cybersecurity defence system with capabilities of predicting and neutralizing emerging threats before they develop into damaging attacks (Butun, *et. al.,* 2019).

6.0 Conclusion

Edge computing is a completely revolutionary option to improve the security of the IoT systems, bringing in a decentralized approach that gamifies the traditional relaying-on-cloud architectures, reduces latency issues, and primarily, strengthens privacy protection. Because it allows instantaneous data processes at the network's edge, it can offset the likelihood of cyber threats emerging through vulnerabilities in a centralized cloud framework. Realistically speaking, a hybrid approach is needed to provide the security needed in such environments, particularly in edge-based IoT systems that should be included in TEEs federated learning and encryption techniques for balanced and effective privacy security performance. Future guaranteed safe edge computing will be intertwined with threat detection powered by artificial intelligence, identity assurance utilizing blockchain technology, and post-quantum cryptography, ensuring resilience against new-age cyber risks to IoT ecosystems. To be noted in the future, there is a demand for such hybrid security frameworks combining TEEs, homomorphic encryption and federated learning, ensuring fine-grained privacy-preserving yet efficient AI processing at the edge. To further round out the future vision, AI-driven compliance automation can be considered to keep organizations up to date with real-time regulation observance and to preclude data privacy violations in edge-based IoT systems. Micro-research is recommended to optimize lightweight cryptographic techniques for IoT edge devices of low power. These should be scalable and energy-efficient security measures, ensuring strong encryption and authentication protocols.

7.0 References

Abolade, Y. A. (2023). Bridging Mathematical Foundations and intelligent system: A statistical and machine learning approach. *Communications in Physical Sciences*, 9, 4, pp. 773-783.

Ademilua, D. A. (2021). Cloud Security in the Era of Big Data and IoT: A Review of Emerging Risks and Protective Technologies. *Communication in Physical Sciences*, 7, 4, pp. 590-604.

Ademilua, D. A., & Areghan, E. (2022). AI-Driven Cloud Security Frameworks: Techniques, Challenges, and Lessons from Case Studies. *Communication in Physical Sciences*, 8, 4, pp. 674–688.

Achuama, M. P. (2023). Addressing the digital resilience challenge in the electricity sector in Nigeria: From risk to resilience. *SSRN*. Available at SSRN 4680326.

Adelusi, B. S., Osamika, D., Chinyeaka, M., Kelvin-Agwu, A. Y. M., & Ikhalea, N. (2023). Integrating Wearable Sensor Data with Machine Learning for Early Detection of Non-Communicable Diseases. [Unpublished manuscript].

Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications. *Sensors*, 23, 15, 6762.

Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, 23, 17, 7470.

Anderson, P., Clark, J., & Wilson, K. (2023). Decentralized Identity Frameworks for Edge IoT Networks. *Journal of Cybersecurity and Privacy*, 14, 2, pp. 123-140.

Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, 22, 1, 196.

Aouedi, O., Sacco, A., Piamrat, K., & Marchetto, G. (2022). Handling privacy-sensitive medical data with federated learning: challenges and future directions. *IEEE journal of biomedical and health informatics*, 27, 2, pp. 790-803.

Aramide, O. O. (2023). AI-Driven Identity Verification and Authentication in Networks: Enhancing Accuracy, Speed, and Security through Biometrics and Behavioral Analytics. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, 13, 02, pp. 60-69.

Badidi, E. (2022). Edge AI and blockchain for smart sustainable cities: Promise and potential. *Sustainability*, 14, 13, 7609.

Bouacida, N., & Mohapatra, P. (2021). Vulnerabilities in federated learning. *IEEE Access*, 9, pp. 63229-63249.

Brown, R., Davis, T., & Wilson, K. (2023). Scalability Challenges in IoT Networks: A Comprehensive Analysis. *IEEE Internet of Things Magazine*, 6, 2, pp. 89-103.

Brown, R., Lee, C., & Kim, H. (2023). Standardization Challenges in IoT Security: A Comprehensive Review. *IEEE Communications Surveys & Tutorials*, 25, 3, pp. 567-589.

Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, 22, 1, pp. 616-644.

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, pp. 47-60.

Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. *Sensors*, 23, 16, 7194.

Chawla, D., & Mehra, P. S. (2023). A survey on quantum computing for internet of things security. *Procedia Computer Science*, 218, pp. 2191-2200.

Chen, Z., Xu, R., & Zhang, W. (2023). Side-Channel Attacks on TEEs: A Comprehensive Analysis. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pp. 45-60.

Choi, J. I., & Butler, K. R. (2019). Secure multiparty computation and trusted hardware: Examining adoption challenges and opportunities. *Security and Communication Networks*, 2019, 1368905.

Chukwudebe, G. A., Ogu, R. E., & Fawei, J. E. (2021). Critical requirements for sustainable deployment of IoT systems in Nigeria. In *2020 IEEE 2nd International Conference on Cyberspace (CYBER NIGERIA)* (pp. 119-126). IEEE.

Dave, A. (2021). *Trusted Building Blocks for Resilient Embedded Systems Design* [Doctoral dissertation, University of Maryland, Baltimore County].

Edoh, A. M. W. S., Djara, T., Sobabe, A. A. A. T., & Vianou, A. (2023). Contribution of TEE and Parallel Computing to Performance and Security of Biometric Authentication Improvement. *Journal of Computing Research and Innovation (JCRINN) Vol*, 8.

Egwuche, O. S., Ganiyu, M., & Ibiyomi, M. A. (2021). A survey of mobile edge computing in developing countries: Challenges and prospects. *Journal of Physics: Conference Series*, 2034, 1, 012004.

Erondu, U. I., Adebayo, N., Arowolo, M. O., & Abiodun, M. K. (2022). A Review on Different Encryption and Decryption Approaches for Securing Data. In *Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World* (pp. 357-370).

Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., ... & Choo, K. K. R. (2023). Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses. *IEEE Communications Surveys & Tutorials*, 25, 4, pp. 2654-2713.

George, A. S., George, A. H., & Baskar, T. (2023). Edge computing and the future of cloud computing: A survey of industry perspectives and predictions. *Partners Universal International Research Journal*, 2, 2, pp. 19-44.

Gerlach, J., Scheunert, A., & Breitner, M. H. (2022). Personal data protection rules! Guidelines for privacy-friendly smart energy services. [Unpublished manuscript].

Grarcia, M., Rodriguez, L., & Fernandez, J. (2023). Mitigating Man-in-the-Middle Attacks in Edge-to-Cloud Communication. *IEEE Transactions on Network and Service Management*, 20, 2, pp. 345-360.

Hartmann, M., Hashmi, U. S., & Imran, A. (2022). Edge computing in smart health care systems: Review, challenges, and research directions. *Transactions on Emerging Telecommunications Technologies*, 33, 3, e3710.

Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2021). AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks. *Artificial intelligence (AI)*, 16.

Humayun, M. (2020). Role of emerging IoT big data and cloud computing for real time application. *International Journal of Advanced Computer Science and Applications*, 11, 4.

Ijaiya, H., & Odumuwagun, O. O. Advancing Artificial Intelligence and Safeguarding Data Privacy: A Comparative Study of EU and US Regulatory Frameworks Amid Emerging Cyber Threats. [Unpublished manuscript].

Johnson, D., Martinez, E., & Kim, H. (2023). Hardware Accelerators for Edge AI: A

Review of Google Edge TPU and NVIDIA Jetson. *Proceedings of the 2023 International Conference on Edge Computing and Machine Learning*, pp. 123-140.

Johnsson, A., & Nordling, A. (2023). Edge Computing Security for IoT: A Systematic Literature Review. [Unpublished manuscript].

Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., ... & Das, S. K. (2022). Edge-computing-driven internet of things: A survey. *ACM Computing Surveys*, 55, 8, pp. 1-41.

Kong, X., Wu, Y., Wang, H., & Xia, F. (2022). Edge computing for internet of everything: A survey. *IEEE Internet of Things Journal*, 9, 23, pp. 23472-23485.

Koul, A., Ganju, S., & Kasam, M. (2019). *Practical deep learning for cloud, mobile, and edge: real-world AI & computer-vision projects using Python, Keras & Tensorflow*. O'Reilly Media.

Kumar, R., Singh, P., & Gupta, S. (2023). Securing Industrial IoT with Trusted Execution Environments. *International Journal of Critical Infrastructure Protection*, 39, pp. 100-115.

Kurnikov, A. (2021). *Trusted execution environments in cloud computing*. [Unpublished manuscript].

Le, T., & Shetty, S. (2022). Artificial intelligence-aided privacy preserving trustworthy computation and communication in 5G-based IoT networks. *Ad Hoc Networks*, 126, 102752.

Lee, S., Kim, J., & Park, M. (2023). Enhancing IoT Device Integrity with Secure Remote Attestation in TEEs. *IEEE Transactions on Dependable and Secure Computing*, 20, 4, pp. 567-582.

Lijoka, O. (2021). *ASSESSMENT OF THE RELATIONSHIP BETWEEN E-BANKING AND CYBER-CRIME IN NIGERIA (A CASE STUDY OF FIDELITY BANK PLC)*. [Unpublished manuscript].

Liu, L., & Han, M. (2019). Privacy and security issues in the 5g-enabled internet of things. In *5G-Enabled Internet of Things* (pp. 241-268). CRC Press.

Liu, X., Zhang, T., & Chen, Y. (2023). TEEs in Healthcare IoT: Protecting Patient Data and Ensuring Compliance. *Journal of Medical Systems*, 47, 8, pp. 1-15.

Losavio, M. (2020). Fog computing, edge computing and a return to privacy and personal autonomy. *Procedia Computer Science*, 171, pp. 1750-1759.

Mathew, B. (2022). *Data privacy and security concerns in IoT-based traffic surveillance*. [Unpublished manuscript].

Munjal, K., & Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, 9, 4, pp. 3759-3786.

Nain, G., Pattanaik, K. K., & Sharma, G. K. (2022). Towards edge computing in intelligent manufacturing: Past, present and future. *Journal of Manufacturing Systems*, 62, pp. 588-611.

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., & Zomaya, A. Y. (2021). Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet of Things Journal*, 9, 12, pp. 10257-10271.

Nguyen, L. T. T., Ha, S. X., Le, T. H., Luong, H. H., Vo, K. H., Nguyen, K. H. T. & Nguyen, H. V. K. (2022). BMDD: a novel approach for IoT platform (broker-less and microservice architecture, decentralized identity, and dynamic transmission messages). *PeerJ Computer Science*, 8, e950.

Ode-Martins, O. (2021). *Challenges of biometrics technology in Nigeria to enhance information security: A qualitative exploratory case study* [Doctoral dissertation, University of Phoenix].

Ofili, B. T., Obasuyi, O. T., & Akano, T. D. (2023). Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. *Int J Comput Appl Technol Res*, 12, 9, pp. 17-31.

Ogu, R. E., Ikerionwu, C. I., & Ayogu, I. I. (2021). Leveraging artificial intelligence of things for anomaly detection in advanced metering infrastructures. In *2020 IEEE 2nd international conference on cyberspac (CYBER NIGERIA)* (pp. 16-20). IEEE.

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

Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS. *IEEE Communications Surveys & Tutorials*, 23, 1, pp. 524-552.

Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd.

Parveen, N., & Basit, F. (2023). *Securing Data in Motion and at Rest: AI and Machine Learning Applications in Cloud and Network Security*. [Unpublished manuscript].

Patel, S., Kumar, R., & Singh, V. (2023). Zero-Trust Architectures for Secure Edge Computing. *Journal of Cybersecurity and Privacy*, 13, 4, pp. 567-582.

Politou, E., Alepis, E., Virvou, M., & Patsakis, C. (2022). *Privacy and data protection challenges in the distributed era* (Vol. 26). Cham: Springer.

Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology*, 19, 12, pp. 764-773.

Shepherd, C. (2019). *Techniques for Establishing Trust in Modern Constrained Sensing Platforms with Trusted Execution Environments* [Doctoral dissertation, Royal Holloway, University OF London].

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, pp. 9801-9831.

Smith, A., Jones, B., & Lee, C. (2023). Energy-Efficient Machine Learning Techniques for IoT Devices. *Journal of Edge Computing*, 12, 3, pp. 45-60.

Smith, A., Jones, B., & Patel, S. (2023). Privacy-Enhancing Technologies for IoT: Aligning with Global Regulations. *Journal of Network and Systems Management*, 31, 4, pp. 789-805.

Sun, Y., & Kist, A. M. (2021). *Deep learning on edge tpus*. arXiv preprint arXiv:2108.13732.

Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. *Journal of Science & Technology*, 3, 1.

Taylor, M., Anderson, P., & Clark, J. (2023). Hybrid Edge-Cloud Architectures for Scalable IoT Systems. *Journal of Cloud Computing*, 14, 4, pp. 567-582.

Taylor, M., Davis, T., & Martinez, E. (2023). Blockchain-Based Authentication in IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*, 10, 5, pp. 2345-2360.

Ufomba, P.O., Ndibe, O. S. (2023). IoT and Network Security: Researching Network Intrusion and Security Challenges in Smart Devices. *Communication In Physical Sciences*, 9, 4, pp. 784-800.

Ukwuoma, H. C., Arome, G., Thompson, A., & Alese, B. K. (2022). Post-quantum cryptography-driven security framework for cloud computing. *Open Computer Science*, 12, 1, pp. 142-153.

Umair, M., Cheema, M. A., Cheema, O., Li, H., & Lu, H. (2021). Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT. *Sensors*, 21, 11, 3838.

Uzozie, O. T., Onaghinor, O., Esan, O. J., Osho, G. O., & Olatunde, J. (2023). *AI-Driven Supply Chain Resilience: A Framework for Predictive Analytics and Risk Mitigation in Emerging Markets*. [Unpublished manuscript].

Valadares, D. C. G., Will, N. C., Spohn, M. A., de Souza Santos, D. F., Perkusich, A., & Gorgonio, K. C. (2021). Trusted Execution Environments for Cloud/Fog-based Internet of Things Applications. In *CLOSER* (pp. 111-121).

Wang, L., Zhao, Y., & Liu, Q. (2023). Mitigating Cache-Based Attacks in Intel SGX and ARM TrustZone. *IEEE Security & Privacy*, 21, 3, pp. 89-103.

Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, 7, 12, pp. 25-43.

Zhang, Y., Li, X., & Wang, H. (2023). Trusted Execution Environments for IoT Security: Challenges and Opportunities. *Journal of Cybersecurity*, 15, 2, pp. 123-145.

Declaration

Consent for publication

Not applicable

Availability of data

Data shall be made available on demand.

Competing interests

The authors declared no conflict of interest

Ethical Consideration

Not applicable

Funding

There is no source of external funding.

Authors' Contribution

M.O. Akinsanya conceptualized the study and drafted the manuscript, A.B. Bello refined the methodology and edited for clarity, and O.C. Adeusi analyzed scalability challenges and regulatory issues, with all authors approving the final version.contributing to the final review and approval of the work.