International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**8**, pp.**21-29**, August **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

A Model for Enhancing Security and Privacy in Pervasive Computing using Homomorphic Encryption

Taylor Onate Egerton[1], Davies Isobo Nelson[2]*

[1,2]Dept. of Computer Science/Faculty of Science, Rivers State University, Port-Harcourt, Rivers State, Nigeria

**Corresponding Author:*

Received: 22/Jun/2025; **Accepted**: 24/Jul/2025; **Published**: 31/Aug/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i8.2129

Abstract: Pervasive computing seamlessly integrates computational capabilities into everyday environments, enhancing user experiences while simultaneously exposing systems to critical security and privacy risks. These vulnerabilities such as unauthorized access, data interception, and exploitation of device-level weaknesses demand encryption methods capable of preserving data confidentiality even during active computation. This paper proposed a novel security model built on Fully Homomorphic Encryption (FHE), enabling operations on encrypted information without decryption, thus ensuring privacy during its lifecycle. The model is structured into a four layered architecture comprising of data collection, encryption, encrypted computation (cloud/edge), and decryption. The study utilized Brakerski/Fan-Vercauteren (BFV) scheme and implemented it using Microsoft SEAL library with VB.NET and C++ for secure, exact integer arithmetic. An experimental evaluation was conducted across 10 to 50 simulated devices using synthesized smart environment data. Experimental finding showed developed model achieved a security accuracy of 95.8%, privacy loss of just 0.6%, and a processing overhead of 720ms, confirming its effectiveness and scalability. To further validate the performance of the developed HE model, a detailed comparative analysis was conducted against that of the traditional cryptographic techniques including AES, RSA, and ECC. While the developed HE model incurs higher computational overhead, it outperformed all baseline methods in terms of security accuracy and privacy preservation. Specifically, the developed HE model showed the lowest privacy leakage and highest resistance to unauthorized access, making it more suitable for sensitive applications despite the trade-off in processing speed. The empirical results highlight the model's strong potential for deployment in real-world domains such as smart cities, healthcare systems, and the Internet of Things (IoT). However, future work should focus on optimizing the model through hybrid FHE–lightweight encryption combinations and integration with real-time IoT protocols.

Keywords: Cryptography, Homomorphic Encryption, Elliptic Curve Cryptography, Microsoft SAEL, Internet-of-Things, Pervasive Computing Environment

1. Introduction

The rise of pervasive computing systems where sensors, mobile devices, and embedded systems continuously collect and exchange information has transformed the technological landscape [1]. However, pervasive environments are highly susceptible to data breaches, privacy violations, and unauthorized surveillance due to their ubiquitous, open, and distributed nature [2]. As a result, network services and smart devices lack protection, compromising personal privacy and making it inconvenient to use [3]. Nonetheless, in recent years, cybersecurity practices is deemed vital for protecting the safety, integrity, and secrecy of communication, assets, and data (both in-transit and at-rest) in electronic environments created by Government, organizations, or any individual using information systems [4].

However, in a time and era of pervasive digital technology, robust data storage and security are essential [5]. Due to the fact that traditional security methods are at risk due to the rising digitization of sensitive data [6]. Existing encryption mechanisms frequently fail to meet the demands of pervasive systems, where data must be processed even in encrypted states. This gap highlights a critical need for innovative solutions that can ensure data integrity and confidentiality.

Homomorphic Encryption (HE) has emerged as a promising approach, allowing computations on encrypted data without decryption [7]. This technique enables computations to be performed on ciphertexts, producing an encrypted data that, when decrypted, matches the outcome of actions executed on the plaintext [8]. By enabling the analysis of sensitive information without exposure, Homomorphic Encryption

(HE) ensures that data remains secure while still being accessible for processing. This capability is especially valuable in situations where sensitive information must be examined without being revealed. HE holds significant promise for enhancing data safety and preserving confidentiality across various applications, particularly within pervasive computing systems. [9].

The purpose of this study is to explore the application of Homomorphic Encryption (HE) in enhancing the security of pervasive computing systems. We aim to address the challenges posed by traditional encryption methods and demonstrate how HE can effectively safeguard sensitive data while enabling necessary computations. This research is motivated by the urgent need for improved cybersecurity practices that protect the safety, integrity, and confidentiality of information in increasingly complex digital environments.

1.1 Objectives of the study

This paper propose a Homomorphic Encryption-based model that enhances privacy while maintaining computational utility. The objectives are to.

i. **Evaluate Security Risks:** Analyze current security risks by identifying privacy vulnerabilities in pervasive computing environments,
ii. **Prevent Data Leakage:** Implement strategies to prevent unauthorized leakage during data transmission or at-rest.
iii. **Design a Secure Model:** Develop a model that leverages Homomorphic Encryption (HE) to facilitate secure, privacy-preserving computation across distributed devices.

The study aim to tackle pressing security concerns in pervasive computing by examining the root causes of its security and privacy vulnerabilities. This study seeks to enhance data security and privacy in distributed environments, ultimately contributing to safer digital interactions.

1.2 Organization

This paper is organized into the following sections which are as follows; Section 1 contains the introduction of the study regarding the subject title, challenges or research problem, and the lay down objectives. Section 2 contains the related works done on the subject matter. Section 3 contains security and privacy challenges related to the subject title and the proposed architecture workflow. Section 4 contains the proposed model and its essential steps in achieving the objectives. Section 5 contains the methodology employed together with the implementation of the study. Section 6 contains the results achieved and discussions of the study. Section 7 contains the comparative analysis with regards to other cryptographic methods. Section 8 concludes the research work with future directions.

2. Related Work

Pervasive computing is the availability of computing on any devices, anyways. Researchers introduced a new paradigm in in this field called “consensus-awareness” that leverages group theory and co-processing. Their approach incorporates bio-engineered sparse connectivity into a consensus mining algorithm. Simulation experiments using group sensing and random number generators in a temperature conditioning scenario demonstrate their method's effectiveness in uncovering novel patterns from uncertain data [10].

Information System (IS) researchers presented an Adaptive Hybrid Case-Based Neuro-Fuzzy System (HCBNFS) for implementing a robust Intrusion Detection and Prevention System (IDPS). Their HCBNFS used Case-Based Reasoning (CBR) to detect known traffic patterns and employed Neuro-Fuzzy Logic as a tuning factor to investigate unknown traffic. Their model was trained with the CIC-IoT2022 dataset and achieved 99% accuracy in intrusion detection and recorded 99.5% for precision, recall, and F1-Score. This empirical evaluation validates their model's effectiveness, enhancing data confidentiality, privacy, and security in IoT-based smart home networks against cyber threats [11].

An innovative framework for Human-Computer Interaction in Pervasive Learning Environments was presented by researchers in response to the shift in educational paradigms toward ubiquitous computing. They used mixed methodologies to develop their framework, which comprises four interconnected layers. Their work was assessed in various academic contexts and demonstrated significant improvements, including a 28% increase in task completion rates, 98% prevention of unauthorized access, and a 23% enhancement in knowledge retention [12].

Research has shown that privacy concerns grow as data collection expands in scale and scope. Traditional encryption (AES, RSA) only secures data at rest or in transit but fails during processing [13]. However, various studies have explored homomorphic encryption in cloud computing, but limited application exists in pervasive computing scenarios [14]. Recently, the field of pervasive computing has garnered significant attention due to its potential for transforming how we interact with technology in everyday environments [15]. Researchers in their study explored the safekeeping and confidentiality problems inherent in these systems, emphasizing the need for robust protective measures [16].

Research paper presented a comparative analysis of modern cryptography techniques, specifically AES, DES, and RSA. The comparison was focused on computation time, memory usage, and safety level. A simulation program was developed for this analysis, and the results indicated that the AES outperforms the other algorithms in all evaluated parameters, making it the superior choice for cryptographic applications [17].

However, in recent years, an Enhanced Homomorphic Encryption (EHE) model to improve data privacy and security was proposed by cybersecurity researchers. Their model incorporated a camouflage process and substitution-based key generation. The proposed EHE optimized encryption and decryption times, significantly outperforming Rivest-Shamir-Adleman (RSA) and standard Homomorphic

Encryption (HE), with processing times of 11 seconds compared to 12 seconds for RSA and 250 seconds for HE [18].

Recent studies focus on enhancing security in distributed cloud environments through innovative protocols. Their notable contributions include a two-layer cryptographic algorithm that integrates genetic techniques for improved encryption with a symmetric-key block cipher that boost complexity [19].

Research author introduced a Hybrid Homomorphic Encryption (HHE) technique that combines symmetric and homomorphic encryption to address privacy challenges. The proposed GuardAI framework enables encrypted data classification on resource-constrained devices while preserving input data and AI model privacy. HHE is demonstrated in heart disease classification using ECG signals, achieving low computational costs and accuracy similar to unencrypted methods [20].

Study introduced Hybrid Homomorphic Encryption to Machine Learning field and proposed a resource-friendly Privacy-Preserving Machine Learning (PPML) protocols for edge devices. They assess the performance of these protocols by assessing communication and computational costs on a dummy dataset, demonstrating their efficiency compared to similar protocols using plain BFV. Finally, they validated the real-world applicability of their construction by developing a PPML application that classifies heart disease using sensitive ECG data, showcasing HHE's effectiveness [21].

Researchers proposed a Lightweight Cryptosystem (LWC) designed as a plugin to safeguard data transmissions in IoT devices and pervasive computing. They utilize various straightforward measuring techniques and implement the system on a Field-Programmable Gate Array (FPGA) board using Verilog to showcase its fitness for real-world security applications [22].

The distinct security challenges associated with cloud, edge, and quantum computing was examined by research authors. Their paper addresses privacy concerns related to data collection, processing, and compliance with regulations like GDPR and CCPA. To tackle these issues, they explore methods like the Zero-Trust Architectures, Privacy-Enhancing Technologies (PETs), and Post-Quantum Cryptography [23].

Authors explored cryptography method to enhance privacy and security in computing environments. Their study emphasizes that the ECC offers robust security with smaller key sizes compared to traditional methods and evaluates its performance in safeguarding information transfer at the edge of IoT networks. Experimental results show ECC achieves an average throughput of 5 Mbps and low latency in encryption and decryption (0.7 and 0.6 milliseconds), enabling efficient data processing at edge devices [24].

Researchers investigated the effectiveness of encryption algorithms using Histogram Analysis, Adjacent Pixel Autocorrelation Test (APAT), and Key Sensitivity Tests. By combining chaos theory, DNA sequence operations, and a redefined hash function, their approach modifies pixel spatial relationships, minimizes information duplication, and enhances responsiveness to changes. The integration of these tests within a chaos-based framework strengthens image encryption, addressing vulnerabilities and ensuring robust protection against attacks. Results show a significant reduction in correlation coefficients (0.85 to 0.05) and entropy values (7.2 to 6.1), while maintaining high visual quality and resistance to various attacks [25].

Research study proposed a cryptographic technique, particularly the hybrid approach of Fully Homomorphic Encryption (FHE) with ECC and PRE (Proxy Re-Encryption) to enhance data security in fog computing. Their results highlight ECC's efficiency, achieving encryption times of 6.5ms for 80-bit security and low latency in decryption, outperforming RSA in both speed and resource requirements. Their study points to promising future directions for improving encryption efficiency and developing robust access control policies for IoT devices in fog environments [26].

An all-inclusive security framework for ensuring secrecy, integrity, and legitimacy of data communication in IoMT ecosystems was proposed by [27]. At the physical layer, they employed AES-256 encryption and HMAC hashing to reduce anomalies and prevent unauthorized access. The additional computational cost is negligible compared to the significant security benefits gained. Findings confirm the feasibility of this security model in protecting diverse healthcare architectures from ongoing cyber threats.

This body of work sets the foundation for our proposed model, which aims to leverage Homomorphic Encryption to improve safety and confidentiality in pervasive computing.
This section will review key contributions in the areas of pervasive computing security, traditional encryption methods, and the advancements in homomorphic encryption, establishing the context for our proposed model.

3. Security and Privacy Vulnerabilities in a Pervasive Computing Environment

Pervasive or ubiquitous computing signifies a shift in how interconnected devices integrate into daily life, creating intelligent environments that anticipate user needs [28]. This environment enables technology to be embedded in various forms, thereby enhancing efficiency and user experiences across different domains such as smart homes, healthcare, and urban infrastructure. Central to this ecosystem is a middleware, which facilitates communication between diverse devices and applications [29]. However, its environment are associated with several vulnerabilities that can compromise security and privacy. The key vulnerabilities of a pervasive computing environment include:

i. Data Breaches: In a digital era, safeguarding sensitive data is of top priority paramount to everyone involved

in the use of information system. This is due to the fact that an unauthorized access to sensitive information can lead to significant privacy violations [30].

ii. Insecure Communication: In a pervasive environment, data in transit are often exposed due to lack of encryption [31]. This vulnerability can expose sensitive information to be intercepted by unauthorized parties, leading to data breaches and privacy violations [32]. Therefore, ensuring secure communication protocols is essential for protecting user data and maintaining trust in pervasive computing applications [33].

iii. Weak Authentication: Insufficient authentication mechanisms may allow unauthorized devices to connect and access sensitive information [34]. This could lead to attack of various forms including brutal-force, observation, and guessing attacks [35].

iv. Interoperability Issues: Vulnerabilities leading to privacy and security issues in a pervasive ecosystem are often linked with diverse standards of smart devices [36]. This can create major vulnerabilities issues or threats.

v. User Unawareness: In a pervasive environment, many users may not realize how much personal information is being gathered or how it is utilized by applications and services. Absence of awareness could lead to unintended privacy breaches, as users may unknowingly consent to data practices that compromise their security [37]. Therefore, increasing transparency and providing clear information about data practices are crucial for empowering users and protecting their privacy in pervasive computing ecosystems [38].

4. Proposed Model

This study presented a model for enhancing security and privacy in a pervasive environment using Full Homomorphic Encryption (FHE). Our objectives are:

i. Ensure privacy-preserving computing in distributed devices,

ii. Prevent unauthorized data leakage during data transmission or processing.

iii. Integrate seamlessly with existing pervasive system including IoT, Mobile Computing, and Sensor Networks.

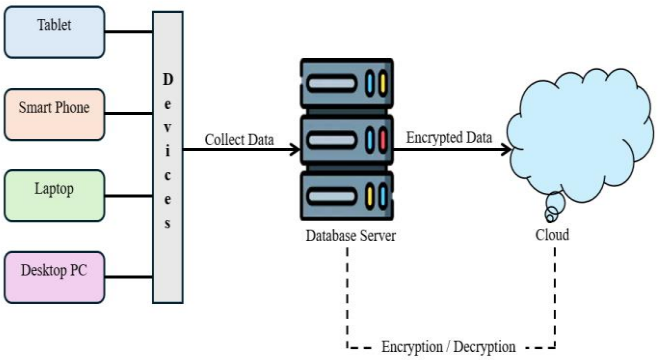
The architecture of our proposed model consists of four (4) layers:

i. Data collection Layer: Responsible for gathering data (e.g., location, biometrics, activity logs) from smart devices.

ii. Encryption Layer: Responsible for encrypting the data using HE before it will be transmitted.

iii. Computation Layer (Cloud/Edge): Responsible for performing computations on encrypted data.

iv. Description Layer: Responsible for decrypting the results only from an authorized receiver.



The workflow begins with devices encrypting their collected data using a public homomorphic key. The encrypted data is sent to the cloud server for processing, where computations are performed directly on the encrypted data. The decrypted results are returned to the client using their private key.

5. Methodology and Implementation

This study utilized Homomorphic Encryption (HE) as the cryptographic technique for the proposed model, allowing computations on encrypted data without need for decryption, thereby and thereby safeguarding its confidentiality throughout the data lifecycle. Additionally, in this study, the middleware plays a crucial role in managing data flows between smart devices and the cloud, ensuring efficient and secure handling of encryption and decryption processes.

The study adopted the Brakerski/Fan-Vercauteren (BFV) scheme implemented via Microsoft SEAL, which supports both additive and multiplicative homomorphism. The proposed model operates on the ring-based lattice cryptography structure to ensure post-quantum security.
Note, the focus of this study is primarily on employing Fully Homomorphic Encryption (FHE) to improve privacy and security. Its operations are based on mathematical structures, including the following:
Let:

$\mathbb{Z}_q$: Ring of integers modulo q, the ciphertext modulus.

$\mathbb{R}_q = \frac{\mathbb{Z}_q[x]}{(x^n+1)}$: Polynomial ring with modulus q and polynomial degree n, where n is a power of 2.

t: Plaintext modulus.

$m \in \mathbb{Z}_t$: The Plaintext message.

Key Generation Step:

Generate secret key: $sk \in \mathbb{R}_q$.

Public key: $pk = (a, b = -a \cdot sk + e)$, where $a \in \mathbb{R}_q$ is uniformly random and e is sampled from a discrete Gaussian distribution χ

Encryption Step:

Given a plaintext m, encode $m \longrightarrow m(X) \in \mathbb{R}_t$.
To encrypt we perform this following:

i. $u \leftarrow \chi$

ii. $e_1, e_2 \leftarrow \chi$

We utilized the following equation to compute the encrypted ciphertext:

$$c_0 = a \cdot u + e_1 + \Delta \cdot m, \quad c_1 = b \cdot u + e_2 \tag{1}$$

Where $\Delta = \left\lfloor \frac{q}{t} \right\rfloor$.

Thus, the ciphertext $c = (c_0, c_1) \in \mathbb{R}_q^2$

Homomorphic Operations

Let $c^1 = (c_0^{(1)}, c_1^{(1)})$ and $c^2 = (c_0^{(2)}, c_1^{(2)})$ be two ciphertexts from different smart devices.

For performing addition operations, we employed the following equation below:

$$c_{add} = (c_0^{(1)} + c_1^{(2)},\ c_1^{(1)} + c_1^{(2)}) \tag{2}$$

For performing multiplication operations, we utilized the equation below:

$$c_{mult} = (c_0', c_1', c_2') = PolyMul(c^{(1)}, c^{(2)}) \tag{3}$$

This results in a three-part ciphertext. To bring it back to a two-part form, re-linearization is performed using evaluation keys.

Decryption:

Given ciphertext $c = (c_0, c_1)$, and secret key sk:

$$m' = \left\lfloor \frac{t}{q} . (c_0 + c_1 \cdot sk) \bmod q \right\rceil \bmod t \tag{4}$$

Here, $m' \in \mathbb{Z}_t$ is the recovered plaintext.

Workflow of the proposed model in a Pervasive Environment

i. **Device Encryption:** Data m from a sensor (e.g., heart rate) is encrypted: $Enc(m) = (c_0, c_1)$

ii. **Cloud Processing:** On ciphertext:
$$Enc(m_1) \cdot Enc(m_2) \Rightarrow Enc(m_1 \cdot m_2)$$

iii. **Client Decryption:** Compute plaintext from result
$$m = Dec(c)$$

5.1 Security Assumptions and Parameters

i. **Noise budget:** Decreases with each operation. This must be managed to prevent decryption failure.

ii. **Security level:** We adopt 128-bit classical security with 4096-bit polynomial modulus and plaintext modulus $t = 65537$.

iii. **Error distribution:** Discrete Gaussian with deviation $\sigma \approx 3.2$

5.2 Implementation Details

The proposed HE model was implemented using the Microsoft SEAL library, specifically leveraging the Brakerski/Fan-Vercauteren (BFV) scheme. The BFV scheme was chosen over the Cheon-Kim-Kim-Song (CKKS) scheme because, although CKKS allows approximate real-number arithmetic, our model requires exact computations on discrete data values commonly found in pervasive computing environments. BFV excels in this context by providing precise integer arithmetic modulo t, thereby eliminating approximation errors and ensuring computational accuracy for security-critical operations.

The development was achieved using C++ with integration into VB.NET, and the backend was supported by Azure Cloud Services. We simulated our dataset using synthesized smart home and mobility logs. For evaluation, we employed various tools, including PowerShell scripts, the SEAL CKKS analyzer, and the Visual Studio Profiler.

6. Results and Discussion

This section presents and interprets the experimental results obtained from the developed model across 10 to 50 devices, as shown in Table 1 and Figures 1-3 respectively.

TABLE 1. Simulated Result Summary

Devices	Security Accuracy (%)	Privacy Loss (%)	Overhead (ms)
10	40.1	3.7	310
20	61.2	2.8	420
30	75.4	1.9	530
40	87.6	1.2	610
50	95.8	0.6	720

Figures 1, 2, and 3 captured the Security Accuracy, Privacy Loss, and Processing Overhead vs. Number of Devices respectively.

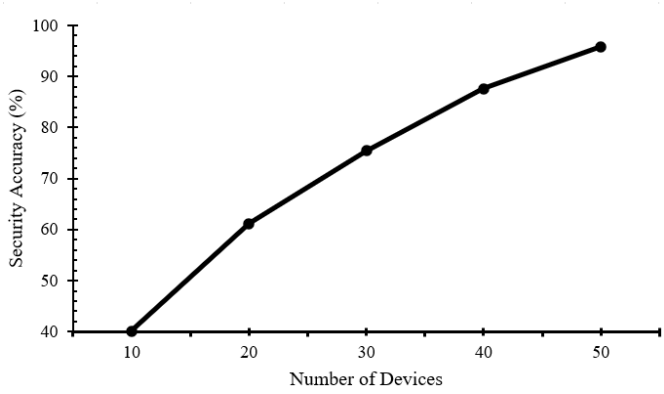


Figure 1: Security Accuracy vs Number of Devices

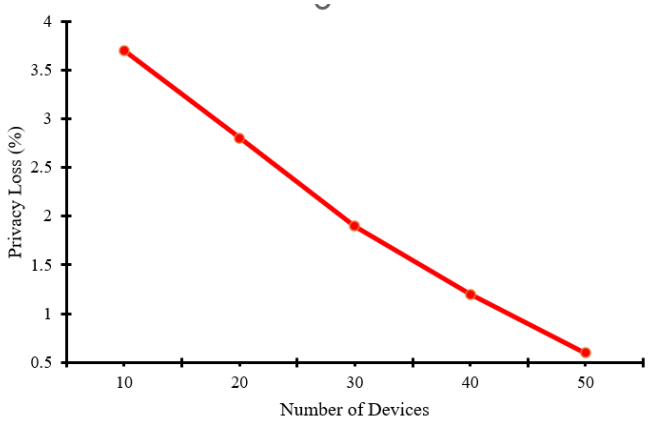


Figure 2: Privacy Loss vs Number of Devices

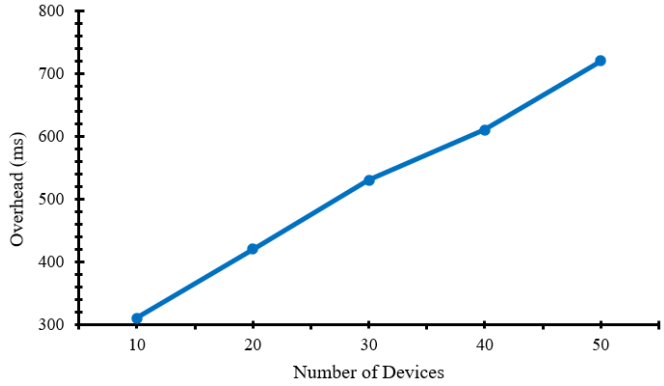


Figure 3: Processing Overhead vs Number of Devices

6.1 Security Accuracy

In this study, the security accuracy metric assesses the model's ability to detect and mitigate unauthorized access attempts or breaches. As the number of devices increased, security accuracy improved significantly, from 40.1% with 10 devices to 95.8% with 50 devices. This trend demonstrates the model's scalability and adaptive security capabilities in handling multiple devices in a distributed setting.

The increasing accuracy with device count is attributed to the richer pool of encrypted interactions enabling better enforcement of access control policies and threat identification mechanisms. This result confirms the developed model robustness in large-scale deployments such as smart cities or industrial IoT systems, where numerous devices generate vast encrypted datasets for secure processing.

6.2 Privacy Loss

The developed model's privacy loss was measured using Shannon entropy-based techniques to evaluate information leakage during encrypted computations. The results revealed a steady reduction in privacy leakage from 3.7% (10 devices) to only 0.6% (50 devices). This reduction correlates with increased entropy in ciphertext distribution and minimized pattern recognition due to homomorphic operations. This means the model effectively obscures sensitive data structures.

Furthermore, in real-world applications such as financial institution or healthcare, where confidentiality is critical, the developed model can support privacy-sensitive data analytics without compromising user trust.

6.3 Processing Overhead

The computational overhead grew linearly from 310 ms (10 devices) to 720 ms (50 devices). This growth is expected due to the added cost of secure operations on encrypted data, which is a known limitation of homomorphic encryption. However, while overhead is higher compared to traditional encryption methods, the use of Microsoft SEAL's BFV scheme and optimized ciphertext packing strategies helped in maintaining acceptable performance levels.

Nonetheless, for time-sensitive environments, this trade-off may not be ideal. However, in use cases where privacy takes precedence over real-time responsiveness, such as medical diagnostics or financial auditing, this overhead is justified.

6.4 Performing Trends

The line graphs in Figures 1-3 demonstrate clear linear trends. Figure 1 shows a sharp rise in security accuracy with increased device count, validating the model's robustness. Further, the line graph in Figure 2 displayed a downward slope in privacy loss, highlighting the model's effectiveness in preserving user anonymity. Finally, Figure 3 reveals the increasing overhead, confirming the known trade-offs of homomorphic encryption.

Collectively, these charts affirm that the model balances security, privacy, and performance, with trade-offs leaning in favor of stronger data protection.

7. Comparative Analysis with Other Cryptographic Techniques

To validate the effectiveness of our proposed Homomorphic Encryption (HE) model, we compared its performance with widely used cryptographic techniques such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC). Based on our experimental results, we focused the analysis on key metrics such as Security Accuracy, Privacy Loss, and Processing Overhead (see Table 2 and Figure 4).

The developed HE model significantly outperforms AES, RSA, and ECC in security accuracy and privacy preservation, achieving a 95.8% accuracy when tested with 50 devices. This high accuracy underscores the model's effectiveness in preventing unauthorized access and maintaining data integrity during computation.

The privacy leakage measured in our experiments was minimal at 0.6% for 50 devices. This indicates that the model effectively preserves user privacy while allowing necessary computations. However, trade-off was evident in processing overhead, where the HE incurs 720ms, as compared to 110-230ms in traditional methods.

Note, despite higher overhead, the uncompromised privacy and computation on encrypted data such as financial data makes our proposed, HE suitable for sensitive and high-assurance pervasive computing systems. The summary results of the comparative analysis conducted is tabulated in Table 2. While Figure 4 captures the bar chart representation of our comparative analysis.

Table 2. Comparative Analysis

Cryptographic Technique	Security Accuracy (%)	Privacy Loss (%)	Processing Overhead (%)
AES	82.3	5.1	110
RSA	78.4	6.2	230
ECC	89.1	3.4	150
Proposed HE	**95.8**	**0.6**	**720**

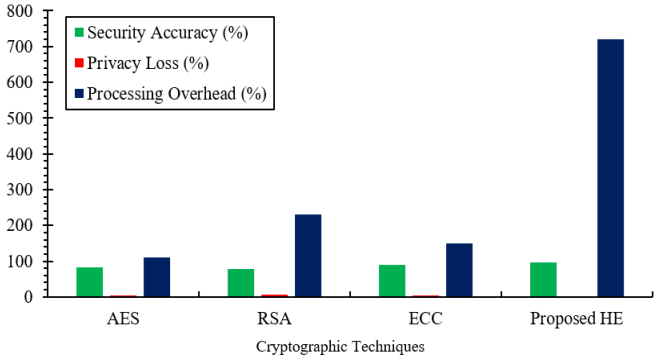


Figure 4: Comparison of Cryptographic Techniques

The results of our proposed FHE model demonstrate its potential to significantly enhance security and privacy in pervasive computing environments, particularly compared to traditional encryption methods like AES, RSA, and ECC.

While the processing overhead of FHE is considerable at 720ms, the trade-offs in security accuracy and minimal privacy loss make it a compelling option for applications requiring secure data processing.

8. Conclusion

This study introduced a technically sound and scalable model based on Fully Homomorphic Encryption (FHE) to address the safety and confidentiality issues of pervasive computing environments. The proposed model was designed to mitigate risks such as data breaches, insecure communications, and weak authentication. Leveraging the Brakerski/Fan-Vercauteren (BFV) scheme, the model ensures end-to-end confidentiality, preserving the privacy of user data even during active processing.

Structurally, the model comprises four integral layers: a data collection layer responsible for acquiring raw input from smart or IoT-enabled devices; an encryption layer that secures the collected data using FHE; a computation layer that performs secure operations in a cloud or edge computing environment; and a decryption layer that ensures only authorized clients can access the results. This architecture supports seamless integration into existing pervasive computing ecosystems, including smart cities, mobile platforms, and healthcare systems.

The model was implemented using the Microsoft SEAL library and deployed through Azure Cloud Services, with VB.NET handling client-side logic. Simulation tests were conducted using synthesized datasets that mimicked real-world pervasive computing applications, such as smart home automation and mobility tracking. Results from these simulations revealed that the model achieved a high security accuracy of 95.8% when deployed across 50 devices, while maintaining a minimal privacy loss of just 0.6% and a manageable processing overhead of 720 milliseconds.

To further validate the efficacy of the proposed solution, a comparative analysis was conducted against other widely adopted cryptographic techniques such as AES, RSA, and ECC. The comparison showed that while AES and RSA provided lower processing overheads, they exhibited higher privacy loss (5.1% and 6.2% respectively) and lower security accuracies (82.3% and 78.4%). ECC performed slightly better in accuracy at 89.1% and privacy loss at 3.4% but still lagged the proposed HE model. In contrast, the proposed HE-based system outperformed all alternatives in terms of both security and privacy metrics, confirming its superior ability to safeguard sensitive data even in open and distributed environments.

Despite the relatively higher computational cost of homomorphic encryption, the privacy-preserving advantages it offers make it highly suitable for privacy-sensitive and security-critical pervasive applications. The trade-off between computational load and data protection was found to be acceptable in many use cases, especially in sectors such as finance, healthcare, smart grids, and distributed mobile systems where data confidentiality cannot be compromised.

Finally, this study contributes a technically robust and practically implementable model that addresses pressing concerns of data security and privacy in pervasive computing, positioning Homomorphic Encryption as a viable foundation for building secure and intelligent ubiquitous systems. However, future work should include real-world deployment of the model in case-specific domains such as e-health and intelligent transportation to assess long-term operational viability. Additionally, integrating lightweight cryptographic methods alongside FHE could further reduce processing overhead, enabling the system to support real-time communication protocols like MQTT and CoAP in resource-constrained environments.

Acknowledgements
We would like to express our gratitude to the various reviewers for their valuable comments that improved the overall manuscript.

Funding Source
All authors confirm that the study conducted was not supported or funded by any external source.

Authors' Contributions
Author-1 researched current trends in related literatures and conceived the study. He also formulated the research questions, objectives, methodology, and refine the theoretical framework.
Author-2 involved in the research development, system design, implementation, and analysis of experimental results and interpretations.
All authors reviewed and edited the manuscript and approved the final version of the manuscript.

Conflict of Interest
All authors declare that they do not have any conflict of interest.

References

[1] J. Agarkhed, G. Pawar, "Enhanced Security Model for Pervasive Computing Using Machine Learning Techniques," *In the Preceeding of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, pp.**414-420**, **2021.**

[2] Y. Jiang, M. A. Rezazadeh Baee, L. R. Simpson, P. Gauravaram, J. Pieprzyk, T. Zia, *et al.*, "Pervasive user data collection from cyberspace: Privacy concerns and countermeasures," *Cryptography*, Vol.**8**, Issue**.5,** pp.**1-5**, **2024**.

[3] K. M. Pradhan, "Pervasive Computing: A New Horizons," *International Journal of Computer Science and Engineering*, Vol.**7**, pp.**1137-1140**, **2019**.

[4] M. A. I. Mallick, R. Nath, "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments," *World Scientific News*, Vol.**190**, pp.**1-69**, **2024**.

[5] E. I. Egho-Promise, M. Sitti, "Big data security management in digital environment," *American Journal of Multidisciplinary Research & Development (AJMRD)*, Vol.**6**, pp.**01-34**, **2024**.

[6] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," *Int. J. Comput. Sci. Mob. Comput.*, Vol.**13**, pp.**88-92**, **2024**.

[7] E. Mollakuqe, A. Parduzi, S. Rexhepi, V. Dimitrova, S. Jakupi, R. Muharremi, *et al.*, "Applications of Homomorphic Encryption in Secure Computation," *Open Research Europe*, Vol.**4**, pp.**158**, **2024**.

[8] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. Fitzek, N. Aaraj, "Survey on fully homomorphic encryption, theory, and applications," *In the Proceedings of the 2022 IEEE International Conference,"* Vol.**110**, pp.**1572-1609**, **2022**.

[9] W. Ren, X. Tong, J. Du, N. Wang, S. C. Li, G. Min, *et al.*, "Privacy-preserving using homomorphic encryption in Mobile IoT systems," *Computer Communications*, Vol.**165**, pp.**105-111**, **2021**.

[10] O. Taylor, P. Asagba, B. Eke, "A Consensus-Aware Pervasive Computing Systems Model for Smart Space Environments," *Journal of Advances in Mathematical & Computational Sciences*, Vol.**7**, pp.**1-8**, **2019**.

[11] I. N. Davies, O. E. Taylor, V. I. E. Anireh, E. O. Bennett, "Adaptive Hybrid Case-Based Neuro-Fuzzy Model for Intrusion Detection and Prevention for Smart Home Network," *International Journal of Computer Sciences and Engineering*, Vol.**10**, pp.**01-10**, **2024**.

[12] O. E. Taylor, I. N. Davies, "A Framework for Human Computer Interaction (HCI) in Pervasive Learning Environment," *International journal of Computer Applications*, Vol.**187**, pp.**26-33**, **2025**.

[13] S. Zubair, H. M. Ahmed, "An In-Depth Comparative Analysis of Cryptographic Techniques for Ensuring Data Privacy in E-Applications," *Paper Presented at the 2024 3rd International Conference for Advancement in Technology (ICONAT)*, pp.**1-8**, **2024**.

[14] S. Kumar, S. K. Singh, B. B. Gupta, K. Psannis, J. Wu, "Homomorphic Encryption in Smart City Applications for Balancing Privacy and Utility," *Innovations in Modern Cryptography*, ed: IGI Global, pp.**241-269**, **2024**.

[15] S. Zhu, T. Yu, T. Xu, H. Chen, S. Dustdar, S. Gigan, *et al.*, "Intelligent computing: the latest advances, challenges, and future," *Intelligent Computing*, Vol.**2**, pp.**6-10**, **2023**.

[16] O. Layode, H. N. N. Naiho, G. S. Adeleke, E. O. Udeh, T. T. Labake, "Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information," *International Journal of Applied Research in Social Sciences*, Vol.**6**, pp.**1193-1214**, **2024**.

[17] O. E. Taylor, V. T. Emmah, "Comparative Analysis of Cryptographic Algorithms in Securing Data," *International Journal of Engineering Trends and Technology*, Vol.**58**, pp.**118-122**, **2018**.

[18] A. H. K. Roseline, N. D. Nwiabu, O. E. Taylor, V. Anireh, "Solving Time Complexity Issues in Storage Area Network using Enhanced Homomorphic Encryption," *International Journal of Computer Science and Mathematical Theory (IJCSMT)*, Vol.**10**, pp.**73-82**, **2024**.

[19] R. R. Asaad, S. R. Zeebaree, "Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms," *Academic Journal of Nawroz University*, Vol.**13**, pp.**476-488**, **2024**.

[20] M. A. Jalil, "Enhancing Privacy in Artificial Intelligence Services Using Hybrid Homomorphic Encryption," *Babylonian Journal of Artificial Intelligence*, Vol.**2024**, pp.**168-174**, **2024**.

[21] K. Nguyen, M. Budzys, E. Frimpong, T. Khan, A. Michalas, "A Pervasive, Efficient and Private Future: Realizing Privacy-Preserving Machine Learning Through Hybrid Homomorphic Encryption," *In the Preceeding of the 2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC)*, pp.**47-56**, **2024**.

[22] M. Abutaha, B. Atawneh, L. Hammouri, G. Kaddoum, "Secure lightweight cryptosystem for IoT and pervasive computing," *Scientific Reports*, Vol.**12**, pp.**19649**, **2022**.

[23] C. Mendoza, J. Herrera, "Enhancing Security and Privacy in Advanced Computing Systems: A Comprehensive Analysis," *Journal of Advanced Computing Systems*, Vol.**3**, pp.**1-9**, **2023**.

[24] I. Davies, O. Taylor, V. Anireh, E. Bennett, "Node-Level Privacy Preservation Mechanism in Internet-of-Things Network using Elliptic Curve Cryptography," *Journal of Applied Computer Science & Mathematics*, Vol.**18**, pp.**26-36**, **2024**.

[25] O. Taylor, C. Igiri, "Enhancing Image Encryption using Histogram Analysis, Adjacent Pixel Autocorrelation Test in Chaos-based Framework," *International Journal of Computer Applications*, Vol.**186**, pp.**9-18**, **2024**.

[26] A. Murugesan, B. Saminathan, F. Al-Turjman, R. L. Kumar, "Analysis on homomorphic technique for data security in fog computing," *Transactions on Emerging Telecommunications Technologies*, Vol.**32**, pp.**3990**, **2021**.

[27] E. Okpu, O. Taylor, "Analysing the Integration of AES-256 Encryption and HMAC Hashing in IoT Smart Healthcare Systems," *Ci-STEM Journal of Digital Technologies and Expert Systems*, Vol.**2**, pp.**18-24**, **2025**.

[28] A. K. Y. Yanamala, S. Suryadevara, "Adaptive Middleware Framework for Context-Aware Pervasive Computing Environments," *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, Vol.**13**, pp.**35-57**, **2022**.

[29] S. Bansal, D. Kumar, "IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication," *International Journal of Wireless Information Networks*, Vol.**27**, pp.**340-364**, **2020**.

[30] R. Nayak, U. Ghugar, P. Gupta, S. Dash, N. Gupta, "Data Privacy and Compliance in Information Security," *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics*, pp.**17-33**, **2025**.

[31] D. Hahn, A. Munir, V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intelligent Transportation Systems Magazine*, Vol.**13**, pp.**181-196**, **2019**.

[32] P. N. Swanzy, A. M. Abukari, E. D. Ansong, "Data security framework for protecting data in transit and data at rest in the cloud," *Current Journal of Applied Science and Technology*, Vol.**43**, pp.**61-77**, **2024**.

[33] J. Zhang, B. Chen, Y. Zhao, X. Cheng, F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, Vol.**6**, pp.**18209-18237**, **2018**.

[34] C. Wang, Y. Wang, Y. Chen, H. Liu, J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, Vol.**170**, pp.**107118**, **2020**.

[35] J. Mohamed, Z. Ibrahim, M. F. M. Fudzee, S. N. Ramli, "Legibility Impact Factor for Shoulder-Surfing Resistant Authentication Scheme by Visual Perception," *International Journal of Business and Technology Management*, Vol.**6**, pp.**206-213**, **2024**.

[36] M. Rashid, M. M. Haque, W. Wang, "IoT Complexity: Security, Vulnerabilities and Risks," *European Journal of Electrical Engineering and Computer Science*, Vol.**8**, pp.**1-9**, **2024**.

[37] S. Aswathy, A. K. Tyagi, "Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future," *In the Security and Privacy-Preserving Techniques in Wireless Robotics*, ed: CRC Press, pp.**163-210**, **2022**.

[38] S. D. Pasham, "Privacy-preserving data sharing in big data analytics: A distributed computing approach," *The Metascience*, Vol.**1**, pp.**149-184**, **2023**.

AUTHORS PROFILE

Dr. Taylor Onate Egerton earned his B.Sc. in Computer Science from Rivers State University, his MSc from the University of Ibadan, and his PhD from the University of Port Harcourt. He currently serves as an Associate Professor and Lecturer in the Department of Computer Science at Rivers State University, Port-Harcourt, Nigeria. A member of the Computer Professionals of Nigeria (CPN), he has published more than 60 research papers in prestigious local and international journals. His research interests include Distributed Systems and Computer Security.

Dr. Davies Isobo Nelson earned his B.Sc. in Computer Science from Kwame Nkrumah University of Science and Technology in Kumasi, Ghana, in 2013. He completed his M.Sc. and PhD at Rivers State University in Port-Harcourt, Nigeria, in 2019 and 2024, respectively. As a researcher and member of the Computer Professionals of Nigeria (CPN), he has published over eight research papers in both local and international journals. His research interests include Network Security and Artificial Intelligence.

