Privacy-Preserving Techniques in Cloud Computing: The Role of Homomorphic Encryption

IBRAHEEM ADEBAYO YOOSUF
University of Derby

Abstract- Given the potential risks associated with cloud computing, industries handling sensitive information like healthcare, government, and finance, must proactively implement robust data privacy measures to protect their customers and maintain compliance. This article explores homomorphic encryption (HE) as a transformative solution for protecting this sensitive information. It presents homomorphic encryption (HE) as a transformative solution for privacy-preserving cloud environments, enabling secure data outsourcing without revealing plaintext data. We discuss HE's ability to process encrypted data in cloud infrastructures and analyze its computational overhead and scalability limitations, which have hindered its widespread adoption. The paper further evaluates key applications, such as privacy-preserving machine learning, financial fraud detection, and genomic data analysis, where HE is highly advantageous. Compared with other privacy-preserving techniques like secure multi-party computation (SMPC) and trusted execution environments (TEEs), we emphasize HE's unique advantage in balancing data privacy and operational efficiency. Future developments in the field, including advancements in HE schemes and integration with other privacy-preserving technologies like differential privacy and secure multi-party computation, are also considered, offering insights into its potential to become a standard in secure cloud computing.

Indexed Terms- Homomorphic Encryption, Cloud Computing, Privacy-Preserving Techniques, Secure Data Outsourcing, Computational Overhead, Machine Learning, Genomic Analysis, Financial Fraud Detection.

I. INTRODUCTION

Cloud computing has seen exponential growth over the past decade, becoming a backbone for various industries. In 2023, global spending on cloud services was $669 billion, up from $444 billion in 2021 with spending in Software as a Service (SaaS) being the highest section, gulping about $413 billion (Statista, 2023). Global spending on IT services reached approximately 1.5 trillion U.S. dollars, and by 2024, this figure increased to 1.61 trillion U.S. dollars. This growth has led to a significant shift in how sensitive data, such as personal healthcare records, financial transactions, and corporate intellectual property, is stored and processed. The sheer volume of data moving to the cloud brings substantial privacy risks, as data is often stored on third-party servers, potentially exposing it to unauthorized access. The demand for privacy-preserving techniques has grown massively with the cloud's adoption to ensure that sensitive information remains secure even while being processed.

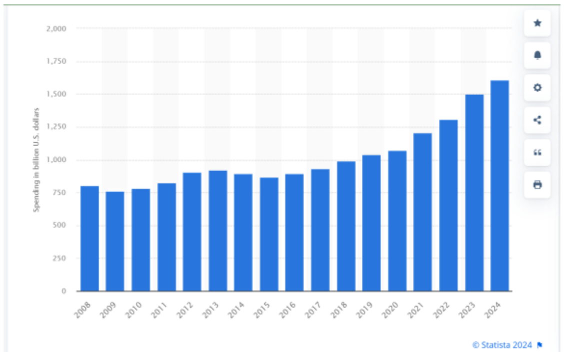

Fig 1: Information technology (IT) services spending forecast worldwide from 2008 to 2024 (in billion U.S. dollars)

Source: Statistica

A major challenge in cloud environments is ensuring privacy while allowing computations to be performed on encrypted data. Traditional encryption methods such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) protect data at rest and during transmission, but they require decryption when performing operations on the data. This decryption moment introduces a vulnerability, exposing sensitive information to potential malicious actors or internal threats from the cloud service provider. As the volume of data grows with projection to reach over 163 zettabytes by 2025 which is 10 times the values of 2016 generated data, finding a secure and efficient method of performing computations without compromising privacy has become a paramount concern for organizations utilizing the cloud (Seagate, 2023).

The objective of this article is to examine the role of homomorphic encryption in enabling privacy-preserving computations in cloud environments. Homomorphic encryption allows computations to be performed on encrypted data without ever decrypting it, preserving privacy and security throughout the computational process. This article will explore how this encryption technique can be applied in cloud computing and analyze its potential to address privacy concerns while also considering its current limitations and practical implications.

Homomorphic encryption offers a promising solution for maintaining data privacy in cloud computing, allowing for secure computations on encrypted data. Although it faces significant challenges, such as computational overhead, slow processing speeds, and scalability issues, it holds great potential to revolutionize privacy-preserving techniques in the cloud. As research continues to refine these methods, homomorphic encryption could become a cornerstone of secure cloud computing practices, allowing organizations to fully leverage the benefits of the cloud while safeguarding sensitive information.

II. LITERATURE REVIEW

Cloud computing has evolved into an important element of modern IT infrastructure, allowing users to store, manage, and process data remotely. According to data from Cloudwards, as of 2024, 94% of enterprises have adopted cloud computing in some capacity, reflecting its widespread integration into business operations. Also, 23% of cybersecurity specialists employ real-time monitoring to assess the security postures of their partners or vendors, emphasizing the increasing concern for security in the cloud ecosystem (Cloudwards, 2024). As organizations increasingly rely on cloud services, concerns regarding data security and privacy have become paramount. One of the primary concerns is data privacy, particularly when sensitive information like biometric data, employee information, healthcare records, financial details, proprietary business data, and the like are entrusted to third-party cloud providers. According to a study by Zulifqar et al. (2022), while cloud computing offers enhanced accessibility and scalability, it also exposes data to risks such as unauthorized access, data breaches, and potential misuse by service providers.

A study by Riggs et al. (2023) highlights the vulnerability of traditional cloud encryption methods. While symmetric and asymmetric encryption techniques, such as AES and RSA, provide secure data encryption during transmission and storage, they fail to protect data during computation, necessitating decryption, which creates a potential attack surface for cybercriminals. In this light, homomorphic encryption has been proposed as a revolutionary solution that can manage these privacy concerns while allowing computations on encrypted data in the cloud.

Homomorphic encryption represents a breakthrough in privacy-preserving techniques for cloud computing. Unlike traditional encryption methods, homomorphic encryption enables computations to be carried out directly on encrypted data without requiring decryption at any point during the process. This unique feature significantly enhances data security by minimizing the risk of exposing sensitive information, even in untrusted cloud environments. A comparative analysis by Stilinki et al. (2024) and Joshi et al. (2022) shows that homomorphic encryption provides superior privacy protection compared to traditional encryption techniques, where data must be decrypted before computation.

Homomorphic encryption is of three primary types, Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), and Fully Homomorphic Encryption (FHE). While PHE allows for limited operations like addition or multiplication and SHE supports a small range of operations, FHE is the most comprehensive form, allowing arbitrary computation on encrypted data. According to Abinaya & Santhi 2021, FHE has significant practical applications, particularly in securely outsourcing private computations. It supports a wide range of operations on ciphertext and can be used an unlimited number of times, offering high flexibility while preserving data privacy, unlike SHE and PHE.

The idea of homomorphic encryption dates back to 1978 when Rivest, Adleman, and Dertouzos first introduced the concept (Casey Crane, 2019). However, early versions were limited to either addition or multiplication, and for many years, the development of a fully functional homomorphic encryption system remained a theoretical challenge. In 2009, a significant breakthrough occurred when Craig Gentry developed the first viable fully homomorphic encryption (FHE) system, based on lattice cryptography. Gentry's scheme demonstrated that it was possible to perform any computation on encrypted data, but the computational overhead was enormous, making it impractical for real-world applications at the time (Gentry, C., 2009).

The computational overhead in Craig Gentry's 2009 fully homomorphic encryption (FHE) system was enormous due to the complex mathematical operations required to maintain encryption during computations. The FHE scheme relied on lattice cryptography, which involved encrypting data to allow computations but significantly increased the size of encrypted data. Each operation added additional noise to the ciphertext, requiring computationally intensive techniques to manage and keep the data usable. This made the process slow and inefficient, limiting its practical application at the time.

Subsequent research has focused on improving the efficiency and practicality of FHE. A study by Halevi and Gentry (2011) introduced batching techniques that allow multiple ciphertexts to be processed simultaneously, reducing the overhead associated with FHE. Similarly, research by Valera-Rodriguez et al. (2024), Yang et. al 2022 and Brand, M., & Pradel, G. (2023) has improved the practical implementation of homomorphic encryption in cloud environments, particularly in areas like machine learning and financial transactions, although the technology still faces challenges regarding scalability and computational costs.

Various studies have explored the practical applications of homomorphic encryption in cloud computing. One of the most researched areas is healthcare, where privacy-preserving techniques are essential for processing sensitive data like genomic sequences. A 2019 study by Yamada, et al. demonstrated the use of FHE for privacy-preserving genomic analysis, allowing researchers to perform computations on encrypted data without exposing sensitive information. In contrast, a study by Valera-Rodriguez et al. (2024) found that while FHE is effective for privacy preservation, its computational inefficiency limits its scalability for large-scale genomic data.

In the financial sector, Nugent, David. (2022) and Yang et. al 2022 showed that homomorphic encryption could be used to perform secure credit scoring and fraud detection without exposing customer data to third parties. However, their findings contrast with the work of Al-Badawi et al. (2020) who argue that the computational overhead of FHE remains a significant barrier to its widespread adoption in financial services. This suggests a trade-off between privacy and performance, a key issue that continues to drive research in this field.

In a typical credit scoring system, customer financial data, such as transaction history, income levels, and credit card usage, are collected and analyzed to assess creditworthiness. Using HE, a financial institution can encrypt the customer's sensitive data before sending it to the credit scoring system. The system, using homomorphic encryption, can perform the necessary calculations—such as aggregating income, calculating debt-to-income ratios, or determining credit card utilization—while the data remains encrypted. For example, banks can apply machine learning models to encrypted datasets to predict credit scores without exposing any personal financial information to third-party service providers.

Fraud detection often involves analyzing transaction patterns to spot unusual activity that might indicate fraudulent behavior. HE allows for the secure analysis of encrypted transaction data. For example, banks can encrypt a customer's transaction history and send it to a cloud-based fraud detection system. The system can then run algorithms, such as Support Vector Machines

(SVMs) or neural networks, on the encrypted data to identify anomalies that may suggest fraud. Since the data is encrypted during this process, neither the cloud provider nor the fraud detection system can access the actual transaction details.

Similarly, in government services, homomorphic encryption particularly Fully Homomorphic Encryption (FHE) has been proposed as a solution for secure electronic to be encrypted and processed without decrypting the data, thereby ensuring voter privacy and protecting against potential breaches during transmission and computation. According to Zhan et al. (2024), FHE's provision of an enhanced layer of security allows computations to be performed directly on encrypted data without needing to decrypt it first making it highly suitable for e-voting systems where voter confidentiality is paramount, ensuring that even third-party cloud servers processing the votes cannot access the actual voting data. This technique is touted as a solution to many privacy concerns in modern electronic voting by preventing unauthorized parties from tampering with or viewing the votes. However, despite the theoretical advantages, the feasibility analysis by Shen (2008) raises concerns about the computational inefficiency of FHE-based systems. The complexity of FHE algorithms results in significantly higher processing times and resource consumption, making real-time vote counting and verification impractical in large-scale elections. One of the main reasons for the computational inefficiency in early FHE systems, like those pioneered by Gentry in 2009, was the process known as "bootstrapping." This technique, which allows for an unlimited number of operations on encrypted data, requires significant computational power due to its complex mathematical operations, including polynomial multiplication and noise management. These operations introduced an enormous computational overhead, making FHE impractical for real-time or large-scale applications during its early development.

Furthermore, the MDPI (2023) study notes that while FHE secures voting data, the computational overhead associated with bootstrapping (a process required to refresh ciphertexts) limits its deployment, particularly in regions with limited computational infrastructure. The scalability of FHE remains a challenge, as large-scale elections require swift and efficient processing, which current FHE implementations cannot provide without considerable latency. Thus, while FHE represents a future direction for securing e-voting, its current limitations in speed and scalability pose significant barriers to widespread adoption in real-world electoral processes.

III. PRIVACY-PRESERVING TECHNIQUES IN CLOUD COMPUTING

Cloud computing offers immense benefits like scalability, accessibility, and cost-efficiency, but ensuring data privacy in such environments remains one of the most significant challenges. When organizations store sensitive data on third-party cloud servers, they essentially place their trust in these external entities, which might lack transparency regarding how data is handled or protected.

In cloud computing environments, privacy concerns remain a top priority due to the nature of data storage and the inherent risks involved. One significant issue is data breaches and unauthorized access. As data is distributed across various geographical locations and managed by different service providers, the likelihood of both external breaches and insider threats rises. Recent studies show that cloud service providers (CSPs) have increasingly become targets for cyberattacks. The multi-layered nature of cloud infrastructure means that a breach in one layer could expose sensitive data stored or processed within that cloud system, a vulnerability that was highlighted by Bisong et al., (2011) in their study on security threats in cloud environments.

Another crucial challenge is the lack of control over data as cloud users, particularly organizations, often surrender a degree of control over how their data is managed when they rely on third-party service providers. As noted by Bamasoud et al. (2020), while CSPs offer sophisticated infrastructure, clients cannot always guarantee that their privacy policies are stringently enforced across the board. This lack of control becomes particularly concerning when dealing with sensitive information, such as personal or financial data, which requires strict compliance with privacy regulations.

A further privacy concern in cloud computing is the multi-tenancy architecture that most cloud platforms adopt. In these architectures, multiple users share the same physical or virtual resources, which can increase the risk of data leakage between tenants. As discussed by Alotaibi et al. (2021), while cloud providers isolate tenants logically, vulnerabilities in the underlying hypervisors or misconfigurations could lead to unintended data access across tenants, exacerbating privacy risks. Multi-tenancy also poses a challenge when trying to enforce uniform security policies across all tenants, each of whom may have different security requirements or compliance obligations (TruOps, 2024).

The culmination of these challenges demonstrates that ensuring privacy in cloud environments is a complex balancing act. Organizations must find ways to protect data without compromising on performance or usability, while also solving the technical and regulatory challenges posed by multi-tenant, distributed cloud systems.

- Existing Privacy-Preserving Methods

Several privacy-preserving techniques have been developed to address data security concerns in cloud environments, but each has limitations, particularly when it comes to the computation of sensitive data. Data anonymization is a widely used method that removes personally identifiable information (PII) from datasets to obscure individual identities. The goal is to maintain the utility of the data while ensuring that sensitive details like names, addresses, or social security numbers cannot be used to identify individuals, thus protecting their privacy while allowing for safe analysis. However, it is vulnerable to re-identification attacks when external datasets are combined. Studies have shown that even when data is anonymized, sophisticated techniques can re-identify individuals, especially in large-scale cloud environments where data is aggregated from multiple sources (Majeed, Abdul & Lee, Sungchang, 2020). This presents a critical challenge for cloud users handling sensitive information, such as in healthcare or finance, where de-anonymization risks are high.

Another approach is differential privacy, which introduces random noise to datasets to mask individual data points while preserving the statistical accuracy of the dataset. Although effective in preventing re-identification, this method can reduce the precision of data, making it less suitable for real-time applications like machine learning, where accuracy is essential (Santanu et al., 2014). The trade-off between privacy and accuracy remains a major challenge for cloud-based systems that rely on precise computations for decision-making processes.

Traditional encryption methods, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), are also used to secure data during transmission and storage. These methods require data to be decrypted before any computations can be performed, exposing it to potential vulnerabilities during the processing phase (Gentry, 2009). This limitation is particularly significant in cloud environments where sensitive operations, such as financial transactions or patient data analytics, need to be processed securely without compromising privacy. While these methods provide varying levels of privacy protection, they do not offer a comprehensive solution for cloud computing, where both data security and computational capabilities are essential. These challenges show the need for more advanced solutions like homomorphic encryption, which allows for computations on encrypted data without exposing sensitive information during processing (Vaikuntanathan, 2011).

- The Unique Role of Homomorphic Encryption

Homomorphic Encryption (HE) offers a transformative approach to the privacy challenges in cloud computing by enabling computations to be performed directly on encrypted data, without requiring decryption. This method addresses one of the key vulnerabilities in traditional encryption: the need to decrypt data for processing. In HE systems, encrypted data (ciphertext) can undergo mathematical operations that produce encrypted results. Once decrypted, these results match the outcome of the same operations performed on the original unencrypted data. This preserves privacy during computation, making it highly useful for scenarios like cloud computing, where data needs to be processed without being exposed to cloud providers (Gentry, 2009).

Homomorphic encryption (HE) offers several key advantages, particularly in cloud computing where privacy concerns are paramount. One of its primary strengths is end-to-end privacy, as data remains encrypted even during computation. This ensures that sensitive information is never exposed, not even to cloud service providers or potential malicious actors. Unlike traditional encryption, which requires decryption for processing, HE enables operations on encrypted data without compromising security (Gentry, 2009). This makes it particularly appealing. HE can be used for securely processing medical records or conducting financial analytics without revealing the buried sensitive information (Al-Riyami et al., 2020; Yamada, et al. 2019).

In addition to privacy, versatility is another advantage of homomorphic encryption. It can be applied across various domains, from secure medical data processing to performing complex financial computations. It is noteworthy to keep in mind that Fully Homomorphic Encryption (FHE) requires immense computational resources, leading to slow processing speeds, especially for large-scale or real-time applications. This computational burden is currently a barrier to its use in time-sensitive or resource-intensive environments (Zhan et al. 2024). Scalability concerns further limit the practicality of FHE. As datasets grow larger, particularly in areas like genomic research or big data analytics, the complexity of FHE becomes a hindrance. While there are ongoing efforts to optimize these systems, achieving efficient large-scale processing remains a challenge (Yamada et al., 2019). The primary solution to the computational limitations of Fully Homomorphic Encryption (FHE) lies in optimizing algorithms and hardware to improve efficiency. Techniques such as leveled FHE (which limits the types of operations) and batching (where multiple data points are processed in parallel) have shown promise in enhancing performance. Additionally, specialized hardware accelerators, like GPUs and FPGAs, are being explored to speed up FHE operations. While these optimizations have improved FHE's feasibility, significant advancements are still required to make it fully scalable for large datasets and real-time applications.

IV. HOMOMORPHIC ENCRYPTION: FUNDAMENTALS AND ADVANCEMENTS

There are three main types of homomorphic encryption which are, Partial, Somewhat, and Fully Homomorphic Encryption (FHE). Partial Homomorphic Encryption (PHE) supports either addition or multiplication operations on encrypted data but not both. Examples include RSA and ElGamal encryption schemes, where only limited computations are feasible. While Somewhat Homomorphic Encryption (SHE) allows a limited number of both addition and multiplication operations. However, the number of operations is restricted by the "noise" in the ciphertext, which grows with each computation. Fully Homomorphic Encryption (FHE) is the most versatile but also the most complex, enabling both addition and multiplication operations to be performed an unlimited number of times on encrypted data, supporting arbitrary computations without decryption (Gentry, 2009).

The mechanics of homomorphic encryption rely on advanced cryptographic techniques that ensure computations can be performed directly on ciphertexts. In FHE, the core idea is to use mathematical structures that allow for the manipulation of encrypted values while preserving their secrecy. Operations like addition and multiplication are applied to encrypted data (ciphertext) and the result, when decrypted, corresponds to the operation applied to the original data (plaintext). In an encrypted database, a user can perform searches or calculations on the encrypted data without ever exposing the data itself. The challenge lies in the "noise" that accumulates during these computations, which can eventually render the ciphertext useless unless carefully managed through bootstrapping techniques. Bootstrapping periodically reduces the noise, enabling more computations (Gentry & Halevi, 2011).

Recent advances in homomorphic encryption (HE) have centered on enhancing computational efficiency and expanding its practical applications across multiple industries. Fully homomorphic encryption (FHE), once thought to be computationally prohibitive, has seen significant performance improvements. Earlier implementations required more resources for even the simplest operations, but recent breakthroughs have managed this issue. A notable example is the development of the TFHE (Torus Fully Homomorphic Encryption) scheme, which focuses on efficiently handling binary circuits. This advancement allows faster computations and makes FHE more practical for proper uses, reducing the time and resource overhead required for complex encryption tasks (Chillotti et al., 2020; Gentry et al., 2009).

In terms of real-world applications, homomorphic encryption is gaining traction in sectors that handle sensitive data, such as healthcare and finance. In healthcare, homomorphic encryption allows for the analysis of sensitive patient data without exposing personal information. Encrypted medical records can be processed to generate treatment insights without compromising patient privacy.

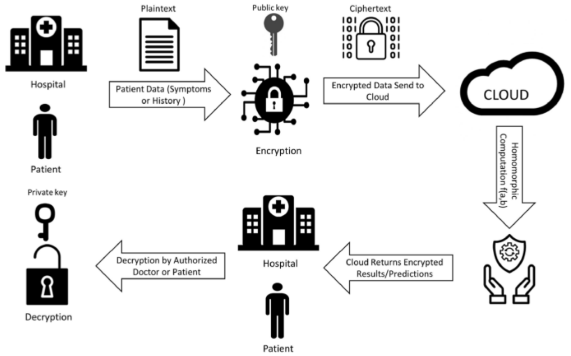
Plaintext
Public key
Ciphertext
Hospital
Patient Data (Symptoms or History)
Encryption
Encrypted Data Send to Cloud
CLOUD
Patient
Homomorphic Computation f(a,b)
Private key
Decryption by Authorized Doctor or Patient
Hospital
Cloud Returns Encrypted Results/Predictions
Decryption
Patient

Fig 2: A systemic review of homomorphic encryption in healthcare

Source: Sprinkler Link

An application of this is observed in a prediction service hosted by Microsoft's Windows Azure for databases in the health sector that are stored in encrypted forms (Yamada et al. 2019; Bos et al., 2014). Microsoft Azure's health sector applications, specifically using Azure Health Data Services, provide robust solutions for processing and analyzing sensitive health data in a secure and compliant way. One prominent feature involves enabling prediction services through the use of homomorphic encryption, which allows data to be processed in encrypted form, protecting privacy even while it is being analyzed.

These services are tailored to help healthcare providers manage sensitive data such as electronic health records (EHRs), clinical trials, and other health-related databases. Microsoft integrates machine learning (ML) and AI capabilities to allow for predictive insights into patient care without exposing sensitive personal information. For instance, a healthcare provider might use Azure's platform to predict patient outcomes or generate treatment recommendations based on encrypted health data stored securely in Azure databases.

This platform also includes Azure API for FHIR (Fast Healthcare Interoperability Resources), which helps in standardizing health data formats, allowing for seamless sharing and interoperability across systems while ensuring regulatory compliance with HIPAA and other healthcare standards.

These advancements represent a growing trend in the healthcare sector towards using cloud-based predictive analytics to enhance patient outcomes, improve operational efficiency, and maintain privacy using encryption techniques like homomorphic encryption.

In the financial sector, FHE has the potential for enhancing secure credit scoring and fraud detection processes, enabling computations on encrypted data without revealing customer information to third parties, thereby preserving confidentiality in financial operations. Moreover, machine learning has also begun integrating homomorphic encryption, allowing models to be trained on encrypted datasets, thus maintaining privacy throughout the machine learning pipeline (Brand & Pradel, 2023).

V. CASE STUDIES

Several case studies highlight the practical application of homomorphic encryption in cloud computing environments. One of the most well-known examples is Google's use of homomorphic encryption to enable encrypted search services. In this system, Google allows users to perform searches on encrypted datasets without decrypting the underlying data (Microsoft, 2022). The search results are computed on the encrypted data and returned in encrypted form, ensuring that neither the search query nor the underlying dataset is exposed to potential breaches.

In addition to Google's implementation, homomorphic encryption has also been employed in financial services for secure data analysis and transaction processing. IBM collaborated with Intesa Sanpaolo, one of Italy's largest banking groups, to implement Fully Homomorphic Encryption (FHE) to enhance secure digital transactions. The use of FHE allows Intesa Sanpaolo to process encrypted data without having to decrypt it first, ensuring that sensitive financial information remains private during transactions. The project was part of a larger initiative to modernize digital security, particularly as cyber threats continue to evolve. The Cybersecurity Lab at Intesa Sanpaolo led this initiative, working with IBM to build systems that securely process encrypted transactions in real time, ensuring that sensitive information remains secure while allowing the bank to continue offering fast and efficient services. This implementation marks a significant step toward using advanced cryptographic techniques in mainstream financial services, positioning Intesa Sanpaolo as a leader in secure digital banking (IBM, 2023). Nugent (2022) explored two machine learning models, XGBoost and a neural network, initially trained on plaintext data and later adapted for encrypted inferences using HE. The research showed that XGBoost significantly outperformed the neural network in terms of speed, achieving encrypted inference in just 6 milliseconds, compared to the neural network's 296 milliseconds. Despite this, the neural network model was identified as more suitable for secure deployments due to its simpler integration process. This case study emphasizes the trade-offs between performance and security when applying HE in financial systems, offering valuable insights into balancing these aspects effectively.

In another study, Núñez et al. (2021) implemented a homomorphic Support Vector Machine (SVM) classifier to enable secure fraud detection in cloud environments. Using lattice-based homomorphic encryption, the researchers demonstrated that financial institutions could outsource fraud detection computations to the cloud without compromising sensitive data. This method ensures that even cloud providers cannot access or infer the details of the data being processed, showcasing the potential of HE to foster privacy-preserving financial systems while leveraging the scalability of cloud computing. These case studies illustrate the versatility and growing applicability of homomorphic encryption across sectors that rely on sensitive data.

VI. CHALLENGES AND LIMITATIONS OF HOMOMORPHIC ENCRYPTION

- Computational Overhead

As earlier discussed, one of the primary challenges of homomorphic encryption (HE) lies in its significant computational overhead. Fully homomorphic encryption (FHE) allows computations on encrypted data without needing decryption, but this flexibility comes at the cost of performance. The encryption, computation, and decryption processes require substantial resources, making FHE slower compared to traditional encryption methods. These high computational costs make it difficult for HE to be applied in real-time applications, particularly in cloud computing, where efficiency is key (Shen 2008; MDPI, 2023). Despite advancements like TFHE which improves efficiency for binary circuits, the technology remains resource-intensive, hindering widespread adoption (Chillotti et al., 2020).

- Scalability Issues

Scalability remains a significant hurdle in deploying homomorphic encryption (HE) in large-scale cloud environments. Processing vast datasets, such as those involved in genomic analysis or financial transactions, requires an immense amount of computing power when encrypted under Fully Homomorphic Encryption (FHE) schemes. While some approaches, like batching techniques such as the Brakerski/Fan-Vercauteren scheme, can manage some scalability issues, real-world deployment for massive datasets remains a challenge. Industries requiring large-scale data analysis, such as the energy sector, and telecommunications, struggle to fully adopt HE technologies, especially when compared to other encryption methods that handle large datasets more efficiently. Furthermore, as the demand for real-time processing grows, HE solutions must adapt to meet the increased computational requirements and provide faster processing times without compromising security. Without addressing scalability, the potential of HE to transform data security in these sectors remains unfulfilled (Microsoft, 2022; Junfeng Fan and

Frederik Vercauteren, 2012; Valera-Rodriguez et al., 2024).

- Security Concerns

Although homomorphic encryption (HE) offers a robust solution for data privacy, it is not without security risks. The complexity of implementing HE systems can introduce vulnerabilities, particularly in poorly optimized or misconfigured environments. Side-channel attacks pose a significant threat, as adversaries can extract sensitive information by analyzing power consumption or electromagnetic emissions during computation. Furthermore, while HE theoretically ensures data confidentiality, its security relies on cryptographic assumptions that may be compromised by advancements in quantum computing. Thus, further research is crucial to enhance HE's resilience against these evolving threats (Bisong et al., 2011; Bamasoud et al., 2020).

- Comparison with Other Encryption Techniques

Compared to other advanced encryption techniques, homomorphic encryption provides unique benefits but also significant trade-offs. Traditional encryption methods, like symmetric encryption, offer fast and efficient data protection but require decryption for any computation, exposing sensitive data to potential breaches during processing. Attribute-based encryption (ABE), another modern encryption method, enables fine-grained access control but still does not allow computations on encrypted data without decryption (Saravana et al. 2015). While Secure Multi-Party Computation (SMPC) distributes computations among multiple parties without revealing inputs, enhancing security but adding communication overhead, Trusted Execution Environments (TEEs) use hardware-based isolation to secure sensitive computations in trusted enclaves, providing faster performance but relying on specific hardware and subject to potential side-channel attacks. In comparing three selective cloud computing tools Amazon Web Services, Microsoft Azure, and Google Cloud Platform, Bahety et al. 2024 concluded none were perfect for all perspectives and arrangements exposing many sorts of gaps between these providers in terms of various attributes. Homomorphic encryption stands out for its ability to perform computations without decryption, but its high resource demands and limited scalability make it less practical for certain real-time and large-scale applications. These trade-offs position HE as a powerful but not universally applicable tool, especially when compared to more computationally efficient alternatives (Stilinki et al., 2024; Joshi et al., 2022; Al Badawi et al., 2020).

VII. FUTURE DEVELOPMENTS IN HOMOMORPHIC ENCRYPTION AND CLOUD COMPUTING

- Potential Improvements

Ongoing research in homomorphic encryption (HE) is focused on enhancing both its efficiency and scalability, addressing the significant computational overhead that currently hinders real-time applications. Researchers are developing optimized schemes like CKKS and TFHE to make computations faster and more efficient for practical use cases. Techniques such as bootstrapping, which refreshes ciphertext to avoid noise accumulation during computations, are being refined to improve the usability of HE in large-scale applications (Chillotti et al., 2020). The growing interest in hardware acceleration, including the use of GPUs and FPGAs, may further reduce the computational load, allowing HE to become more feasible for cloud computing environments. Innovations in lattice-based cryptography, which promotes many HE schemes, also promise to strengthen the security and performance of these encryption methods in the future (Che et al., 2008).

- Integration with Other Privacy-Preserving Technologies

The future of homomorphic encryption lies in its potential integration with other privacy-preserving technologies, such as differential privacy and secure multi-party computation (SMPC). Differential privacy, which adds noise to datasets to prevent the identification of individuals, could complement HE by enhancing privacy protections in data processing without sacrificing accuracy. Meanwhile, SMPC, which allows multiple parties to jointly compute a function over their inputs while keeping those inputs private, can be combined with HE to create more secure privacy-preserving frameworks. These integrations could enable more secure data sharing and processing in cloud environments, particularly in sensitive industries like healthcare and finance. Combining HE with these techniques could create a layered security model that balances privacy, efficiency, and scalability (Shen 2008; Chillotti et al., 2020).

- The Future of Privacy-Preserving Cloud Environments

Advances in homomorphic encryption technology could pave the way for a new era of secure and private cloud computing. As data privacy regulations tighten globally, there is an increasing need for technologies that enable secure and compliant data processing in the cloud. HE's ability to perform computations on encrypted data without revealing the underlying information positions it as a valuable tool for maintaining confidentiality. If ongoing research can overcome its current limitations, HE has the potential to become a standard in privacy-preserving cloud architectures, enabling industries like telecommunications, healthcare, defense, finance, and government to fully outsource their data processing to the cloud without compromising security. The combination of HE with other emerging technologies, such as quantum-resistant cryptography, could further solidify its role in next-generation cloud security (Microsoft, 2022).

CONCLUSION

In conclusion, homomorphic encryption (HE) presents a transformative approach to addressing privacy challenges in cloud computing. Our exploration detailed how HE allows secure data processing without compromising confidentiality, making it essential for sectors handling sensitive information, such as healthcare and finance. However, current limitations, such as computational overhead and scalability issues, impede its widespread adoption. Comparing HE to techniques like Secure Multi-Party Computation (SMPC) and Trusted Execution Environments (TEEs) further reveals that each method offers unique strengths, but HE holds the most promise for future cloud security innovations. Ongoing research into improving efficiency and integrating HE with other privacy-preserving technologies will be essential in ensuring its viability as a standard in cloud computing. Despite its challenges, HE is set to become an increasingly important tool for secure and private cloud-based applications as advancements continue. This work describes the growing potential of HE in ensuring privacy in an ever more cloud-dependent world, where secured data protection is paramount.

REFERENCES

[1] Abinaya B., Santhi S.2021. A survey on genomic data from a privacy-preserving techniques perspective https://www.sciencedirect.com/topics/computer-science/fully-homomorphic-encryption

[2] Al-Riyami, S., & Sprott, M. (2020). Homomorphic Encryption: A Survey on Practical Applications in Cloud Computing. Journal of Cloud Computing, 9(4), 12–30.

[3] Al Badawi, A., Polyakov, Y., Veeravalli, B., & Rohloff, K. (2020). Implementation and Performance Evaluation of RNS Variants of the BFV Homomorphic Encryption Scheme. IEEE Transactions on Emerging Topics in Computing, 8(2), 553-566. DOI: 10.1109/TETC.2019.2911966 https://eprint.iacr.org/2018/589.pdf?ref=blog.sunscreen.tech

[4] Alotaibi, Abeer & AlZain, Mohammed & Masud, Mehedi & Jhanjhi, Noor. (2021). A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 12. 1978-1990.

[5] Alves, S., & Rodrigues, A. (2023). Financial Technology and Financial Inclusion: The U.S. Experience. Journal of Business Research, 147, 245-260. https://doi.org/10.1007/s40747-022-00756-z

[6] Bahety, Ms & Bhushan, Prof & Patil, Dr. (2024). A Comparative Study Of Various Cloud Computing Tools. Journal of Advanced Zoology. 45. 77-81. 10.53555/jaz.v45iS4.4155.

[7] Brand, M., & Pradel, G. (2023). Practical Privacy-Preserving Machine Learning using Fully Homomorphic Encryption. Cryptology ePrint Archive, Report 2023/1320. Available at: https://eprint.iacr.org/2023/1320.

[8] Bisong, Anthony & Rahman, Shawon. (2011). *An Overview of The Security Concerns in Enterprise Cloud Computing*. International Journal of Network Security & Its Applications. 3. 10.5121/ijnsa.2011.3103.

[9] Bos JW, Lauter K, Naehrig M. *Private predictive analysis on encrypted medical dat*a. J Biomed Inform. 2014 doi: 10.1016/j.jbi.2014.04.003.

[10] Casey Crane, 2019. The SSL Store. What is Homomorphic Encryption? [Explained]. Available at: https://www.thesslstore.com/blog/what-is-homomorphic-encryption/#:~:text=The%20Origins%20of%20Homomorphic%20Cryptosystems,the%20concept%20of%20privacy%20homomorphisms. Accessed September 30, 2024

[11] Chillotti, I., Gama, N., Georgieva, M., & Izabachene, M. (2020). "TFHE: Fast Fully Homomorphic Encryption over the Torus." Journal of Cryptology, 33, 34-91. https://eprint.iacr.org/2018/421

[12] Cloudwards.net. (2023). Cloud Computing Statistics: The Latest Numbers and Trends in 2023. Retrieved from https://www.cloudwards.net/cloud-computing-statistics

[13] Cloudwards. (2023). Cloud Computing Statistics: How Cloud Has Changed the World in 2023. Retrieved from https://www.cloudwards.net/cloud-computing-statistics/

[14] Costa, Laécio & Ruy, B & Queiroz, J. (2014). The Use of Fully Homomorphic Encryption in Data Mining with Privacy Preserving.

[15] Craig Gentry, Shai Halevi, Nigel P. 2011 Better Bootstrapping in Fully Homomorphic Encryption Https://eprint.iacr.org/2011/680.pdf

[16] D. M. Bamasoud, A. S. Al-Dossary, N. M. Al-Harthy, R. A. Al-Shomrany, G. S. Alghamdi and R. O. Algahmdi, 2021. "Privacy and Security Issues in Cloud Computing: A Survey Paper," International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 387-392, doi: 10.1109/ICIT52682.2021.9491632.

[17] Fontaine, C., Galand, F. A Survey of Homomorphic Encryption for Nonspecialists. EURASIP J. on Info. Security 2007, 013801 (2007). https://doi.org/10.1155/2007/1380

[18] Gentry, C. (2009). "A Fully Homomorphic Encryption Scheme." PhD Thesis, Stanford University. Available at: https://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf.

[19] Gentry, C. (2009). A Fully Homomorphic Encryption Scheme (Doctoral dissertation, Stanford University). Retrieved from https://crypto.stanford.edu/craig/craig-thesis.pdf

[20] Haoran He, Zhao Wang, Hemant Jain, Cuiqing Jiang, Shanlin Yang. 2022. A privacy-preserving decentralized credit scoring method based on multi-party information, Decision Support Systems https://doi.org/10.1016/j.dss.2022.113910 https://www.sciencedirect.com/science/article/pii/S0167923622001816

[21] IBM. (2023). Intesa Sanpaolo and IBM enable secure digital transactions using fully homomorphic encryption. IBM Blog. Retrieved from https://www.ibm.com/blog/intesa-sanpaolo-ibm-secure-digital-transactions-fhe

[22] Joshi, Bineet & Joshi, Bansidhar & Mishra, Anupama & Arya, Varsha & Gupta, Avadhesh & Perakovic, Dragan. (2022). A Comparative Study of Privacy-Preserving Homomorphic Encryption Techniques in Cloud Computing. International Journal of Cloud Applications and Computing. 12. 1-11. 10.4018/IJCAC.309936.

[23] Junfeng Fan and Frederik Vercauteren (2012). Homomorphic Evaluation of the AES Circuit. Cryptology ePrint Archive, Report 2012/144. Available at: https://eprint.iacr.org/2012/144

[24] Kelly Koeninger, Robinson Bradshaw & Hinson PA, and John Conley. 2020 International Health Data: How HIPAA Interacts with the EU GDPR. University of North Carolina-Chapel Hill and Robinson Bradshaw & Hinson PA. https://www.robinsonbradshaw.com/media/publication/657_International%20Health%20Data.pdf

[25] Majeed, Abdul & Lee, Sungchang. (2020). Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3045700. https://www.researchgate.net/publication/347730431_Anonymization_Techniques_for_Privacy_Preserving_Data_Publishing_A_Comprehensive_Survey

[26] Microsoft. (2022). Genomic analysis on Galaxy using Azure CycleCloud. Microsoft Azure Blog.

Retrieved from https://azure.microsoft.com/en-us/blog/genomic-analysis-on-galaxy-using-azure-cyclecloud/

[27] Microsoft. (2022). Microsoft launches Azure Health Data Services to unify health data and power AI in the cloud. Azure Blog. Available at: https://azure.microsoft.com/en-us/blog/microsoft-launches-azure-health-data-services-to-unify-health-data-and-power-ai-in-the-cloud/

[28] Nugent, David. (2022). Privacy-Preserving Credit Card Fraud Detection using Homomorphic Encryption. 10.48550/arXiv.2211.06675.

[29] Núñez, D., Loureiro, V., Fernández-Pendás, J., & Pérez, A. (2021). Secure Outsourcing of Fraud Detection Using Lattice-Based Homomorphic Encryption. Journal of Network and Information Security, 202

[30] Riggs, Hugo, Shahid Tufail, Imtiaz Parvez, Mohd Tariq, Mohammed Aquib Khan, Asham Amir, Kedari Vineetha Vuda, and Arif I. Sarwat. 2023. "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure" Sensors 23, no. 8: 4060. https://doi.org/10.3390/s23084060

[31] Santanu Basak, Kakali Chatterjee, Ashish Singh, 2023. DPPT: A differential privacy preservation technique for a cyber-physical system, Computers and Electrical Engineering, https://doi.org/10.1016/j.compeleceng.2023.108661. https://www.sciencedirect.com/science/article/pii/S0045790623000861

[32] S. Che, J. Li, J. W. Sheaffer, K. Skadron and J. Lach, "Accelerating Compute-Intensive Applications with GPUs and FPGAs," 2008 Symposium on Application Specific Processors, Anaheim, CA, USA, 2008, pp. 101-107, doi: 10.1109/SASP.2008.4570793.

[33] Saravana Kumar Na ,Rajya Lakshmi G.Vb ,Balamurugan B. (2015). International Conference on Information and Communication Technologies (ICICT 2014) Enhanced Attribute-Based Encryption for Cloud Computing.

[34] Seagate Technology. (2017). Data Age 2025: The evolution of data to life-critical. Retrieved from https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

[35] Statista. (2023). Global spending on public IT cloud services by segment from 2015 to 2023. Retrieved from https://www.statista.com/statistics/370305/global-public-it-cloud-services-spending-by-segment/#:~:text=In%202023%2C%20the%20global%20spending,nearly%20413%20billion%20U.S.%20dollars.

[36] Statista. (2023). Global IT services spending forecast from 2017 to 2025. Retrieved from https://www.statista.com/statistics/203291/global-it-services-spending-forecast/

[37] Stilinki, Dylan & Adablanu, Selorm. (2024). Homomorphic Encryption for Secure Cloud Computing. 10.13140/RG.2.2.19574.41285.

[38] TruOps. (2024). Governance, Risk, and Compliance (GRC) in the Age of Digital Transformation: Enhancing Security and Operational Resilience. TruOps White Paper. Retrieved from https://truops.com/wp-content/uploads/2024/08/TruOps-GRC-White-Paper-8.24.pdf.

[39] Vaikuntanathan, Vinod. (2011). Computing Blindfolded: New Developments in Fully Homomorphic Encryption. Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS. 5-16. 10.1109/FOCS.2011.98.

[40] Valera-Rodriguez, Francisco-Jose, Pilar Manzanares-Lopez, and Maria-Dolores Cano. 2024. "Empirical Study of Fully Homomorphic Encryption Using Microsoft SEAL" Applied Sciences 14, no. 10: 4047. https://doi.org/10.3390/app14104047

[41] Yamada, N., et al. (2019). Evaluating the Scalability of Homomorphic Encryption in Large Genomic Datasets. BITS Journal, 14(3), 342–356.

[42] Yamada, Y., Hanamura, S., & Nakagawa, H. (2019). Practical Privacy-Preserving Data Processing: Fully Homomorphic Encryption's Application to Cloud Environments. BITS2019, Ochanomizu University. Available at: http://ogl.is.ocha.ac.jp/Publications/paper2019/BITS2019_yamada.pdf.

[43] Yang, Yang & Huang, Xindi & Liu, Ximeng & Cheng, Hongju & Weng, Jian & Luo, Xiangyang & Chang, Victor. (2019). A Comprehensive

Survey on Secure Outsourced Computation and Its Applications. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2949782.

[44] Ying, SHEN. (2008). The Feasibility Analysis of Electronic Voting. https://www.mdpi.com/2079-9292/13/2/286

[45] Zhan, Yu, Wei Zhao, Chaoxi Zhu, Zhen Zhao, Ning Yang, and Baocang Wang. 2024. "Efficient Electronic Voting System Based on Homomorphic Encryption" Electronics 13, no. 2: 286. https://doi.org/10.3390/electronics13020286

[46] Zulifqar, Isma & Anayat, Sadia & Kharal, Imtiaz. (2021). A Review of Data Security Challenges and their Solutions in Cloud Computing. International Journal of Information Engineering and Electronic Business. 13. 30-38. 10.5815/ijieeb.2021.03.04.