**Enhancing Security and Privacy of Clients’ Data Stored by Financial Institutions Using Homomorphic Encryption Schemes**

Mallesh Darisi

Jyothi Sai Krishna Ravuri

Venu Linga

Prakash Raj Baskar Raj

Anirudh Tallavajhula

University of Missouri Kansas City

CS 5533 Applied Cryptography

Sravya Chirandas

2023

# **Abstract**

The project aims to investigate implementing homomorphic encryption to enhance the security and privacy of any communication and information shared and transmitted via the cloud. Financial institutions such as banks are moving to the cloud for their data storage and transfer for ease of information management due to the high daily volume of data. The move, however, puts the data of thousands of clients at risk of cyber threats. Thus, it is significant to implement a high-profile cryptographic method to enhance security and privacy. This project aims to apply homomorphic encryption through Quantum mechanisms to better the security and privacy confidentiality of financial data stored in the cloud. A new framework that analyzes quantum cryptography algorithms and homomorphic encryption schemes is designed to improve privacy and security protection in cloud environments. This project aims to provide security and privacy to financial institution client's data stored in the cloud.

*Keywords: Quantum Cryptography, Homomorphic Encryption, Algorithm, Cloud Environment*

Table of Contents

[**Abstract** 2](#_Toc150761769)

[**Introduction** 4](#_Toc150761770)

[**Importance of Data Security and Privacy** 5](#_Toc150761771)

[**Homomorphic Encryption Schemes** 6](#_Toc150761772)

[**Background** 7](#_Toc150761773)

[**Cloud Storage in financial institutions** 8](#_Toc150761774)

[**Benefits of Cloud Storage** 8](#_Toc150761775)

[**Challenges and Risks of Storing Client Data in the Cloud** 9](#_Toc150761776)

[**Literature Review** 10](#_Toc150761777)

[**Cloud Security and Privacy in the Financial Industry** 10](#_Toc150761778)

[**Encryption Schemes and Techniques Used in Financial Institutions** 12](#_Toc150761779)

[**Strengths and Weaknesses of Current Approaches** 13](#_Toc150761780)

[**Problem Statement** 14](#_Toc150761781)

[**Proposed Project Model** 15](#_Toc150761782)

[**Addressing Security and Privacy Issues** 16](#_Toc150761783)

**[Project Architecture](#_Toc150761784)** [1](#_Toc150761784)6

**[Design Flow](#_Toc150761785)** [1](#_Toc150761785)7

[**HES Code for Cloud Data Protection** 1](#_Toc150761786)8

[**Issues and challenges** 19](#_Toc150761787)

[**Exploring Potential Advantages and Disadvantages** 19](#_Toc150761788)

[**Future Developments Potential** 2](#_Toc150761789)1

[**Conclusion**](#_Toc150761787) 22

[**References** 2](#_Toc150761790)3

# **Introduction**

With the technological advancements in recent years, the financial service industry has been dramatically digitalized. Such change has facilitated the enormous growth in the volume of confidential customer information saved in the cloud. This transformation, without doubt, offers a lot of convenience and efficiency, but at the same time, there is an essential problem concerning the security and confidentiality of the data (Susanto et al., 2016). The data security placed on the customers' most secret financial information has become more complicated as financial institutions have to protect it from emerging cyber risks. In response to this threat, the financial sector resorted to state-of-the-art cryptographic solutions, with homomorphic encryption being among the most advanced solutions for ensuring vital confidentiality and privacy of information in a cloud setting.

This has necessitated effective security mechanisms due to integrating cloud computing with finance. Cloud computing is essential today as most financial transactions, like banking and investment management, are digitalized. Nevertheless, it is vital to acknowledge that this revolutionary tech advancement exposes finance to additional points of weakness (Martin et al., 2017). Data breaches, especially those involving the financial sector, have profound implications regarding the substantial monetary losses they cause and their detrimental effect on the credibility of institutions. Financial institutions are obligated to protect client’s confidential documents and information; hence, they must observe extreme care when handling any form of financial data.

As with any other evolving threat in cyberspace, it is imperative to consider a holistic approach towards data security and privacy. Cybercriminals, in particular, are highly sophisticated, using various means, such as malware, phishing, and ransomware, to break into the secured information belonging to the respective financial sectors (Thach et al., 2021). Thus, it creates an environment where conventional security methods may only be partially practical, thus pushing for a new approach to data protection.

## **Importance of Data Security and Privacy**

Data security and privacy remain a central core and nonnegotiable in the financial institution's daily running. Protecting crucial financial information is vital to help support this importance. Financial institutions store sensitive, private information; hence, firstly. This covers clients' primary personal data and sophisticated financial details such as bank account information, stock accounts, transaction history, and identification data (Alloghani et al., 2019). Compromization of this information would be disastrous for those individuals as well as for the institutions involved.

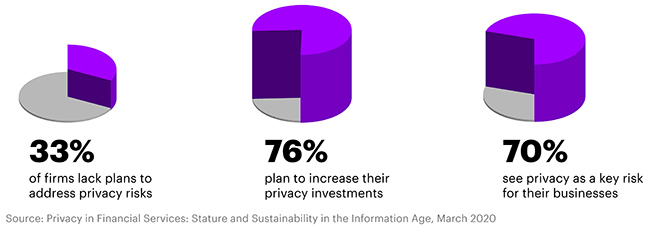


Figure 1: Embracement of privacy as an issue in financial institutions

Secondly, various financial industry regulators, such as FINRA and SEC, set strict rules about protecting sensitive information. These regulations require financial institutions to be proactive about data security and privacy issues (Chen et al., 2017). If an institution does not comply with such standards, it would lead to expensive penalties and harm that particular institution's credibility.

In addition, since we are today living in the era of a digital environment, the same is expected by clients when using internet services for their financial needs. These institutions become repositories of their financial trust, so such private information must remain strictly confidential (Alloghani et al., 2019). Data security breaches or compromises can lead to a loss of trust by customers, thereby propelling them to find other financial services providers. Data security and confidentiality, hence, become not only compliance issues but also critical sources of competitiveness in a market where trust and reputation matter most.

However, maintaining data security and privacy for financial institutions goes beyond complying with regulations and client's expectations. It is also tied to the stability of the financial sector generally. The financial industry is essential in the global economy, and a leak in that sphere is prone to creating ramifications that do not go away from particular firms but from the whole system. Therefore, data security and privacy should be viewed as an institution’s obligation in addition to avoiding broader economic instability.

## **Homomorphic Encryption Schemes**

Homomorphic encryption has thus presented itself as an innovative and viable means for strengthening the security and confidentiality of cloud-based client information used by financial institutions. The mentioned systems represent a new trend in cryptography, which implies an entirely different method for protecting confidential financial data (Rocha et al., 2018). However, a new solution of homomorphic encryption resolves this dilemma. It allows the execution of computation operations on encrypted data while the sensitive data remains protected. In carrying out this idea, we are working with a mathematical operation on the closed box without opening it for inspection. This marks an unparalleled stride forward in cryptography with significant data protection and confidentiality ramifications, particularly in banking.

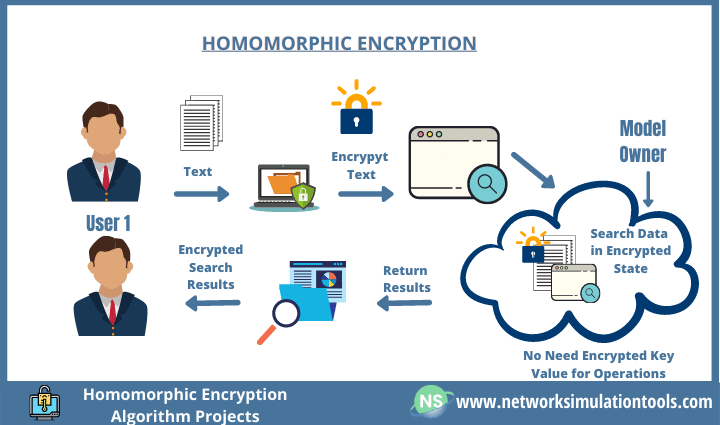


Figure 2: Homographic mechanism

Homomorphic encryption schemes provide an up-to-date solution to ensure data security and privacy during the financial sector’s cloud-based activities. This approach provides for a novel manner of looking at data security for the safe execution of confidential financial operations when in an encrypted form (Rocha et al., 2018). In this article, as further research is carried out, we shall shed light on how homomorphic encryption works in practice, its advantages and disadvantages, and what banks can do to use this modern development.

# **Background**

Cloud computing applications have transformed some financial industries with their growing acceptance rates in the last few years. This section looks into why cloud storage is used by financial institutions, its advantages, as well as risks and difficulties involving storing clients' data on the cloud.

## **Cloud Storage in financial institutions**

Modern financial institutions have made cloud storage one of the essential parts of their IT infrastructure. It entails keeping information in outside servers, which off-site cloud services vendors maintain. The financial industry utilizes cloud storage for many functions, such as simple data backups to CRM, analytics, and regulations. Scalability is one of the significant reasons why financial institutions adopted the cloud storage model (Elzamly et al., 2016). Unlike in the past, institutions today can enjoy unlimited storage space with cloud services as their storage increases or reduces depending on demands. Scalability is essential in the financial sector, where transaction volumes may vary significantly with the market condition, transaction peaks, or seasonal trends. In addition, it allows for portability and convenience. The data in financial institutions can be accessed quickly and securely by authorized users anywhere with internet connectivity. It makes it possible for remote work, working between different geographical locations and, in real-time, accessing all important financial data.

## **Benefits of Cloud Storage**

The adoption of cloud storage by financial institutions brings forth a myriad of benefits:

* Cost Efficiency: Instead of investing vast amounts of money on physical hardware, cloud storage offers more convenience and easy storage. It reduces capital expenditure, and financial institutions can pay as you store.
* Scalability: Cloud platforms are flexible and thus allow scaling up or down depending on the organization's needs.
* Accessibility: Such cloud storage provides easy and secure accessibility of data from any given location, where it encourages collaborative efforts for distant work operations.
* Redundancy and Disaster Recovery: Most cloud providers implement robust data redundancy with a good disaster recovery strategy, thus making the data available amidst hardware failure or catastrophe.
* Security Features: By using cloud providers, data security is made possible using complex security measures such as encryption, access controls, and threat detection.
* Advanced Analytics: Cloud-based analytics allows financial institutions to understand what is hidden in data that could help determine investment decisions, manage risks, and provide insights into customers’ needs.
* Compliance: Cloud providers have compliance certificates (SOC 2, PCI DSS, among others), which are pretty helpful in meeting statute conditions and set regulations.

## **Challenges and Risks of Storing Client Data in the Cloud**

While the adoption of cloud storage in financial institutions offers substantial benefits, it is not without its challenges and risks:

* Security Concerns: It is a concern to store sensitive client data in the cloud using the provided security of the cloud provider. Risks include data breaches and unauthorized access.
* Data Privacy: Financial institutions must work with data privacy laws, including GDPR and CCPA, that could apply to client information retained in the cloud (Elzamly et al., 2016). Compliance is a critical concern.
* Data Transfer Speed: Although there is more accessible access to a large amount of data in the cloud, it could be slower to reach the data than local storage, affecting real-time data processing.
* Vendor Lock-In: A single cloud provider can lead financial institutions to depend on them, making it difficult or even impossible to find another provider or revert to an on-premise solution.
* Downtime: Cloud outages may halt operations, leading to losses, damages, or adverse market perceptions.
* Data Sovereignty: Data sovereignty laws may demand that data be kept in some specified locations, making it less suitable for cloud providers.

These have made it imperative to look for viable means of securing important information stored in the financial institutes' systems. Such is the rationale for this project development to implement a cryptographic mechanism to beef up the existing security mechanisms.

# **Literature Review**

## **Cloud Security and Privacy in the Financial Industry**

Integration of cloud computing platforms in the banking sector has had revolutionary impacts on business efficiency and affordability. On the other hand, this innovation has posed considerable hurdles, with grave worries about protecting confidential financial information. An extensive body of literature on cloud security and privacy in the financial industry summarizes the research, findings, and recommendations. Security and privacy issues relating to cloud adaptation have emerged as a significant theme in the literature. The risk factor is apparent in financial institutions handling personal information such as client's financial records, investment portfolios, and transaction histories. Data breach, among others, is among these risks, with far-reaching effects, including monetary losses and brand dilution.

There is also increased emphasis on regulatory compliance in cloud security and privacy in the banking industry. The SOX, PCI DSS, and GDPR are examples of regulations that force Financial establishments to adhere to strict data protection rules. Hon & Millard (2018) note that researchers have insisted on this position as they call upon cloud operators to bring their offers into consistent conformity, helping financial institutions adjust themselves.

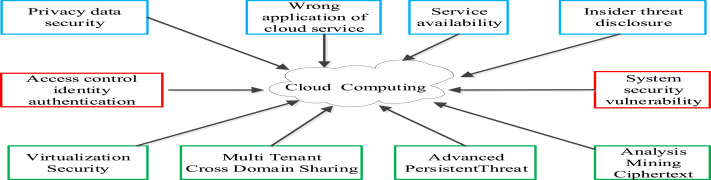


Figure 3: Security and Privacy issues in cloud computing.

Secondly, the literature explores multiple dimensions of cloud security. For example, data encryption plays a vital role in cloud-based security strategies used by modern financial institutions. These studies evaluate numerous encryption approaches involving symmetric and asymmetric encryption and whether they can secure critical financial information (Chenthara et al., 2019). Encryption remains one of the most essential tools for keeping data confidential, especially during transmission or storage inside the cloud platform.

Further, cloud security talks also involve IAM and authentication and authorization methods. Therefore, it should be a priority for management teams to ensure that only authorized staff have access to and can tamper with sensitive monetary records. Researchers have also studied preventing unauthorized access through strong IAM and access control policies in the cloud environment (AL-Hawamleh et al., 2023). The shared responsibility model is another significant characteristic concerning cloud security in the financial industry. The cloud security model lays out the roles of the cloud service providers and financial institutions in ensuring the cloud is safe. The financial institution takes it upon itself to secure its applications and data, while the cloud provider manages infrastructure and physical security (AL-Hawamleh et al., 2023). It is essential to understand this model, define the division of responsibilities, and achieve the comprehensiveness of the security posture.

## **Encryption Schemes and Techniques Used in Financial Institutions**

Encryption is one of the most critical factors in protecting confidential financial information through various security measures used within financial institutions. Literature on financial institutions' encryption schemes and techniques is an all-inclusive sketch of how these bodies safeguard their client's data.

Another popular encryption method used in the financial sector is tokenization. Tokenization refers to replacing confidential information using tokens or proxies such that, even when intercepted, the details remain illegible. Researchers also examined whether tokenization reduces risk and improves compliance, including against PCI DSS (Iezzi, 2020). Different encryption schemes and techniques used in financial institutions present their ability to provide data security, but they have constraints (Miyan, 2017). Fully homomorphic encryption has high computational overheads and is one of the main issues. This might imply real-time data processing due to its strong security guarantees and intense computation characteristics (Iezzi, 2020). Financial institutions must cautiously assess such schemes regarding the security versus performance trade-off.

Additionally, controlling encryption keys and verifying they are safely distributed has been a problem. Management of encryption keys is vital for strong encryption, and lapses in this context can compromise the whole encryption architecture (Alamgir et al., 2017). However, research in this area advocates for strong key management procedures as one of the measures that can be taken to mitigate the possible loopholes. A plethora of literature describes various types of encryption schemes and techniques used for protecting sensitive financial data in banks. Homomorphic Encryption, End-To-End encryption, and Tokenization are new methods financial companies apply to increase their information safety (Alamgir et al., 2017). The techniques discussed here provide very rigorous security against leakage of data and illegal entry. Nevertheless, these are also some of the problems encountered in that section of the literature, such as computational overload, key administration, and balance of security and performance. This creates several challenges for financial institutions to protect client's data, fulfill the relevant regulations, and maintain confidence among the public, especially in the digital era.

## **Strengths and Weaknesses of Current Approaches**

Assessing the pros and cons of existing data security in the banking sector justifies why homomorphic encryption schemes are needed in banks. Financial institutions deal with large amounts of confidential information, which must be secured best without compromising performance. Homomorphic encryption is a possible solution due to the pros and cons associated with existing approaches in the financial industry. The robustness remains one of the significant strengths of current data security techniques used in most financial institutions—diligent use of encryption, access control, and authentication mechanisms for financial information. For example, data encryption guarantees this information would remain confidential if unwarranted access is experienced. This is particularly important for data in motion and resting state in the cloud settings (Lohr et al., 2019). Through the use of access controls and authentication processes, such information should be accessed by only authorized personalities, which, in turn, ensures better data security.

Additionally, most of the recent methods incorporate full IAM frameworks as well. IAM plays a significant role in the management of user identities, the definition of roles, and the introduction of access policies. It supports fine-grained management of authorized users' access rights for financial institutions, thereby minimizing the risk of unauthorized access (AL-Hawamleh, 2023). Nevertheless, they also possess significant weaknesses. Implementing some security measures has led to additional computational costs as one of the significant difficulties encountered during this time. For example, encryption offers privacy for the data but could be slower, primarily when FHE is used (Miyan, 2017). Financial institutions must find a fine line between robust security measures and the best performance possible. Key management poses another challenge. The security of one's information is directly proportional to managing these specific elements known as encryption keys. It is no mean task to ensure the safe distribution of keys, storage, and possible revoking, which require keen observation.

Based on the above-identified security and privacy gaps existing in cloud computing for financial data, it is thus significant to implement a robust homomorphic encryption scheme for handling the issues experienced in financial institutions.

# **Problem Statement**

Financial organizations face significant security and privacy issues when hosting customer data in the cloud. The sensitive nature of the data, which includes financial and personal information, makes it a desirable target for hacking and unauthorized access. The primary security worry is the possibility of data breaches, where hackers exploit loopholes in the cloud architecture and weak authentication procedures to obtain unauthorized access to client data (Rocha et al., 2018). Employees or partners with privileged access may purposely leak or misuse customer information, making insider threats another severe hazard. Such breaches or unauthorized access may have dire repercussions. Financial loss is significant because it can be extremely expensive to investigate and fix the breach, notify impacted clients, offer credit monitoring services, and face potential legal consequences. Another serious repercussion is reputational harm because customers depend on financial organizations to protect their private data. Clientele and revenue loss may result from bad press, diminished credibility, and a ruined brand image. Legal and regulatory repercussions, including prospective legal actions and penalties for inadequate client data protection, are also conceivable. Lastly, customers might require more trust and assurance in the institution's capacity to safeguard their data, impairing its capacity to offer individualized services and undermining its competitive edge (Susanto et al., (2016) It is evident that more sophisticated security methods are necessary to improve data protection despite existing security features being implemented. Financial institutions must address these security and privacy concerns to guarantee the security and privacy of customer data stored in the cloud.

# **Proposed Project Model**

The suggested strategy uses homomorphic encryption techniques to improve the security and privacy of customer data that financial institutions store in the cloud. Homomorphic encryption is a cryptographic method that preserves data confidentiality by enabling computations to be conducted on encrypted data without decryption. Financial companies can overcome the security and privacy concerns related to keeping customer data in the cloud by utilizing the unique characteristics of homomorphic encryption.

Homomorphic encryption offers several benefits for preserving client data confidentiality. The data is protected even as processed in the cloud, ensuring end-to-end encryption. As a result, there is no longer any need to disclose unencrypted data to cloud service providers or other parties participating in the data processing system. Additionally, homomorphic encryption enables financial institutions to carry out various activities on encrypted data without decrypting it, lowering the danger of illegal access. Finally, homomorphic encryption adds a significant layer of defense against insider threats. It prevents workers or partners accessing client data from viewing or altering the actual data because it is encrypted.

# **Addressing Security and Privacy Issues**

The proposed method successfully resolves financial organizations' security and privacy concerns while storing customer data in the cloud. The confidentiality of customer data is protected throughout its lifecycle in the cloud using homomorphic encryption techniques. Because the encrypted data is secure even when accessed by unauthorized parties, data breaches and unlawful access are reduced. Only encrypted data would be discovered by hackers trying to take advantage of loopholes in the cloud architecture or lax authentication procedures, rendering it useless without the decryption key (Hon & Millard, 2018). The suggested method also tackles the insider threat by ensuring that even staff members or partners with access privileges cannot view or change the client data. This extra layer of security dramatically decreases the possibility of data leaks or illegal access from within the financial institution. Financial organizations can execute necessary computations on encrypted data using homomorphic encryption, reducing the requirement to decode sensitive data. As a result, there is a considerably lower chance of data breaches during the processing stage because less plaintext data is exposed. As a result, financial institutions may still take advantage of cloud storage's cost and scalability benefits while maintaining high data security and privacy levels.

# **Project Architecture**

To improve secure data protection, the project needs to meet the following criteria;

* Client-Side Encryption: Client-side encryption encrypts data at the client before it is delivered to the cloud storage. This should be incorporated into the architecture.
* Cloud Infrastructure: A secure cloud infrastructure that follows industry best practices for data security should be part of the project architecture.
* Key Management System: To produce, store, and manage encryption keys securely, a key management system should be implemented.
* Data processing models: The project architecture needs to include modules for data processing that can run calculations on encrypted data using homomorphic encryption techniques.

## **Design Flow**

Figure 4: Project Design Flow

The design flow indicates the flow of the project execution, starting with the need for the financial institutions to use cloud systems to store and transfer data. The primary goal is to use HES cryptography that allows the use of the information without decryption. After identification of the potential problems, the organization should use an additional HES layer to enhance the set security mechanisms.

## **HES Code for Cloud Data Protection**

A screen shot of a computer program

Description automatically generated

A computer screen shot of a program code

Description automatically generated

In this example, we simulate homomorphic encryption by encrypting two integers, multiplying them, and then decrypting the outcome to obtain the sum of the original numbers.

# **Issues and challenges**

## **Exploring Potential Advantages and Disadvantages**

The suggested project's implementation, which aims to improve security and privacy in financial institutions through the use of homomorphic encryption techniques, comes with several clear benefits. In the first place, homomorphic encryption ensures that client data is kept private during its entire lifecycle in the cloud. Financial institutions can regulate the encryption process and ensure that confidential data is secure before being sent to cloud storage by encrypting the data on the client side. This adds another level of protection from data breaches and unwanted access. Second, secure computations on encrypted data are made possible by homomorphic encryption. This reduces the risk of exposing sensitive data during processing because financial institutions can now execute various actions on the data without decryption. Because employees or partners with access to the data cannot view or change it in its decrypted version, this encourages data privacy and reduces the danger of insider attacks. Thirdly, preserving the advantages of cloud storage, such as cost savings and scalability, is a benefit of the project execution. Financial organizations can use cloud infrastructure to store client data while utilizing homomorphic encryption to protect the data's security and privacy. This enables more adaptability and effectiveness in the storing and processing of data.

When implementing this project, several potential drawbacks should be taken into account. First, homomorphic encryption techniques can be computationally demanding and need much processing power. The potential for increased processing time and resource usage could impact the performance of data processing processes. Financial institutions may need to invest in solid hardware or cloud resources to reduce these computing demands. Second, homomorphic encryption necessitates a complete comprehension of the various encryption techniques and their use in practical situations. Financial institutions may need to spend money on specialist knowledge and training to integrate and manage homomorphic encryption in their cloud infrastructure successfully.

Furthermore, using homomorphic encryption can make interoperability more difficult. Compatibility with pre-existing systems and platforms may be restricted since homomorphic encryption techniques are still in their infancy and developing. Financial institutions may need to spend on system updates, integration initiatives, or bespoke development to ensure seamless compatibility and functionality. The effect on data analytics and processing capacity is another possible issue. The kinds of computations and data analysis that can be carried out on encrypted data may be restricted by homomorphic encryption. Some sophisticated algorithms or queries might not be practical or need further thought and adaptation. This could affect the capacity to obtain valuable analysis and insights from the data kept on the cloud.

## **Future Developments Potential**

Performance Optimization: Improving the performance of homomorphic encryption systems is one topic for future work. To reduce processing time and resource needs, research and development activities should concentrate on increasing the computational efficiency of these methods. In order to improve the performance of homomorphic encryption, this can entail investigating novel algorithms, hardware acceleration strategies, or parallel computing.

Industry standards should be established, and compatibility between various encryption techniques and cloud platforms should be encouraged as homomorphic encryption develops further. Standardization would make it easier to integrate homomorphic encryption into current systems, make it compatible with them, and make it possible for financial institutions to collaborate and share data easily.

Usability and User Experience: Future advancements should improve homomorphic encryption's usability and user experience in financial institutions. For the sake of streamlining the encryption and decryption procedures, this includes creating user-friendly interfaces, tools, and documentation. User education and training programs should also be designed to provide staff with the know-how and abilities to use homomorphic encryption efficiently and safely.

Advanced Analytical Capabilities: Research and development efforts should enhance homomorphic encryption's capacity for sophisticated data analytics and calculations. Expanding the operations that may be performed on encrypted data will make it possible to use more complex analytical methods. Financial organizations could do this without jeopardizing the security and privacy of their encrypted data and gain more significant insights from it.

# **Conclusion**

Financial institutions need robust and reliable security mechanisms to enhance their data privacy and security while utilizing a more flexible and cost-efficient cloud system. The proposed project's implementation uses the unique properties of homomorphic encryption, including end-to-end encryption, secure calculations, and defense against insider threats. It enables financial companies to balance using the advantages of cloud storage with maintaining the privacy and integrity of customer data. It is important to note that homomorphic encryption is still a developing technology, and that additional research and development efforts are required to improve its usability, industry standards, and performance. It will also be crucial to make ongoing efforts to overcome interoperability issues and increase the analytical capabilities of homomorphic encryption.

# **References**

Alamgir, M., Campbell, M. J., Sloan, S., Goosem, M., Clements, G. R., Mahmoud, M. I., & Laurance, W. F. (2017). Economic, socio-political and environmental risks of road development in the tropics. *Current Biology*, *27*(20), R1130-R1140.

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *International Journal of Advanced Computer Science and Applications*, *14*(2).

Alloghani, M., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. *Journal of Information Security and Applications*, *48*, 102362.

Chen, Z., Li, Y., Wu, Y., & Luo, J. (2017). The transition from traditional banking to mobile internet finance: an organizational innovation perspective-a comparative study of Citibank and ICBC. *Financial Innovation*, *3*(1), 1-16.

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.

Elzamly, A., Hussin, B., Abu Naser, S., Khanfar, K., Doheir, M., Selamat, A., & Rashed, A. (2016). A new conceptual framework modelling for cloud computing risk management in banking organizations. *International Journal of Grid and Distributed Computing*, *9*(9), 137-154.

Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1–banks' use of cloud services. *Computer law & security review*, *34*(1), 4-24.

Iezzi, M. (2020, December). Practical privacy-preserving data science with homomorphic encryption: an overview. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 3979-3988). IEEE.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

Miyan, M. (2017). FHE Implementation of Data in Cloud Computing. *International Journal of Advanced Research in Computer Science*, *8*(3).

Rocha, V. F., López, J., & Da Rocha, V. F. (2018). An overview on homomorphic encryption algorithms. *UNICAMP Universidade Estadual de Campinas, Tech. Rep*.

Susanto, A., Chang, Y., & Ha, Y. (2016). Determinants of continuance intention to use the smartphone banking services: An extension to the expectation-confirmation model. *Industrial Management & Data Systems*, *116*(3), 508-525.

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845.