Secure financial application using homomorphic encryption

Vijaykumar Bidve[1], Aruna Pavate[2,3], Rahul Raut[4], Shailesh Kediya[5], Pakiriswamy Sarasu[6], Koteswara Rao Anne[7], Aryani Gangadhara[8], Ashfaq Shaikh[9]
[1]School of Computer Science and Information Technology, Symbiosis Skills and Professional University, Pune, India
[2]Thakur College of Engineering and Technology, Mumbai, India
[3]Department of Scientific Research, Innovation and Training of Scientific and Pedagogical Staff, University of Economics and Pedagogy, Karshi, Uzbekistan
[4]School of Computer Science and Information Technology, Symbiosis Skills and Professional University, Pune, India
[5]School of Logistics and Supply Chain Management, Symbiosis Skills and Professional University, Pune, India
[6]Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India
[7]Mukesh Patel School of Technology Management and Engineering, NMIMS, Mumbai, India
[8]Department of F.Y. B.Tech., D. Y. Patil College of Engineering, Pune, India
[9]Department of Information Technology, M. H. Saboo Siddik College of Engineering, Mumbai, India

Article Info

Article history:

Received May 25, 2024
Revised Oct 10, 2024
Accepted Oct 30, 2024

Keywords:

Computational integrity
Confidentiality
Cryptographic techniques
Data security
Financial data protection
Homomorphic encryption

ABSTRACT

In today's digital age, the security and privacy of financial transactions are paramount. With the advent of technologies like homomorphic encryption, it is now possible to perform computations on encrypted data without the need to decrypt it first, offering a promising avenue for secure financial applications. This research paper explores the implementation and implications of utilizing homomorphic encryption in financial applications to safeguard sensitive data while maintaining computational integrity. By employing homomorphic encryption techniques, financial institutions can enhance the confidentiality of their clients' information, protect against data breaches, and enable secure computations on encrypted data. The paper discusses the principles of homomorphic encryption, its applications in financial systems, challenges, and potential solutions. Additionally, it examines real-world examples and case studies where homomorphic encryption has been employed successfully, highlighting its effectiveness in ensuring the privacy and security of financial transactions. Overall, this paper aims to provide insights into the role of homomorphic encryption in creating secure financial applications and its potential to revolutionize the way sensitive financial data is handled and processed.

Corresponding Author:

Vijaykumar Bidve
School of Computer Science and Information Technology, Symbiosis Skills and Professional University
Kiwale, Pune, Maharashtra 412101, India
Email: vijay.bidve@gmail.com

1. INTRODUCTION

The sensitive nature of financial transactions and data makes secure financial consulting essential in the current digital era. Protecting people's assets and stopping fraud requires maintaining the confidentiality, integrity, and privacy of financial information. Traditional approaches to financial data protection, however, frequently compromise usability for security, which creates difficulties for financial institutions as well as their clients [1]-[3]. Homomorphic encryption offers a promising solution to this dilemma by enabling computations to be performed directly on encrypted data, thereby preserving its confidentiality while allowing for meaningful analysis and processing [4]-[6]. In the financial sector, where data privacy regulations are stringent and the need for secure data processing is paramount, homomorphic encryption holds significant relevance. By leveraging homomorphic encryption, financial institutions can perform complex computations on sensitive financial data without the need to decrypt it, thus mitigating the risk of data breaches and unauthorized access while ensuring compliance with regulatory requirements [7]-[9]. This makes homomorphic encryption a valuable tool for enhancing the security and privacy of financial consultancy services, ultimately fostering trust and confidence among clients and stakeholders [10].

Traditional financial consultancy methods typically involve the exchange and processing of sensitive financial data between clients and financial institutions. These methods often rely on encryption techniques to protect data during transmission and storage, but computations on encrypted data usually require decryption, introducing security risks. In contrast, homomorphic encryption, represented by functions such as $E(m1) * E(m2) = E(m1 + m2)$, allows computations to be performed directly on encrypted data without decryption, preserving data confidentiality. This enables financial consultants to analyze encrypted financial data securely, ensuring the privacy of sensitive information [11]. For instance, in loan consultancy, computations such as interest rate calculations and risk assessments can be performed on encrypted loan data using homomorphic encryption formulas, maintaining data confidentiality throughout the process. Similarly, in credit card consultancy, computations involving transaction amounts and fraud detection can be securely executed on encrypted credit card data [12]. Homomorphic encryption thus revolutionizes traditional financial consultancy methods by offering a secure and privacy-preserving approach to data analysis and computation, enhancing trust and confidentiality in financial transactions [13]. One common traditional method involves the use of statistical models and algorithms to analyze financial data and predict future outcomes, such as investment returns or loan defaults. These models often require access to sensitive client information, which must be decrypted for analysis. This decryption process exposes the data to potential security vulnerabilities. However, these computations often require access to plaintext data, making them susceptible to privacy breaches and unauthorized access [14].

Secure financial consultancy leverages advanced cryptographic strategies like homomorphic encryption to ensure the confidentiality and integrity of touchy economic facts. By encrypting statistics earlier than processing, customer records stays stable throughout analysis and computation, mitigating the chance of facts breaches or unauthorized get admission to. This method allows economic experts to perform complex analytics and computations on encrypted records without compromising privateness [15]. Key considerations encompass efficient implementation, strong key control, and ongoing protection tests to maintain the highest standards of safety. Through secure financial consultancy, clients can believe that their monetary facts is safeguarded while nonetheless profiting from precious insights and tips. This modern method now not most effective complements protection but also fosters agree with and self belief in financial offerings, strengthening client relationships and regulatory compliance [16], [17].

As the financial industry continues to adapt, secure financial consultancy plays a crucial role in addressing rising threats and making sure the confidentiality and integrity of financial information. Homomorphic encryption unearths application throughout diverse sectors, together with finance, healthcare, and cloud computing, through allowing computations on encrypted records without decryption [18]. In finance, it guarantees the confidentiality of sensitive financial facts at some point of facts analysis and transactions, improving safety and privateness. Healthcare benefits from homomorphic encryption by way of permitting medical facts analysis while preserving affected person privateness, permitting collaborative studies and customized remedy. In cloud computing, homomorphic encryption allows secure outsourcing of information processing tasks to untrusted servers, protecting records confidentiality and integrity [19]. Overall, homomorphic encryption offers a powerful answer for privacy-maintaining computations in numerous fields, safeguarding touchy information in an an increasing number of interconnected world.

There are certain limitations of this technology including computational complexity: homomorphic encryption imposes sizable computational overhead, doubtlessly slowing down processing speed and responsiveness in monetary transactions and information evaluation. Limited supported operations: current homomorphic encryption schemes help handiest a subset of operations, limiting the forms of monetary computations that may be finished while retaining records privacy [20]. Key management challenges: managing encryption keys securely, inclusive of key era, garage, and distribution, gives logistical and protection demanding situations, in particular in large-scale economic structures. Scalability issues: scaling homomorphic encryption to deal with huge volumes of financial data and complicated computations may also pressure computational assets, memory, and bandwidth, proscribing sensible deployment in actual-global situations. Performance trade-offs: balancing safety and performance requires cautious optimization and change-offs, doubtlessly compromising either statistics privacy or processing efficiency in secure financial programs [21]. Interoperability concerns: lack of standardized protocols and interoperable implementations impedes seamless integration of homomorphic encryption into heterogeneous economic structures, hindering significant adoption. Regulatory compliance complexity: ensuring compliance with regulatory necessities, which includes statistics safety laws and enterprise standards, provides complexity and overhead to implementing homomorphic encryption in economic packages [22]. Ongoing research needs: addressing these boundaries calls for persisted studies and improvement efforts to enhance the performance, scalability, safety, and usefulness of homomorphic encryption for steady financial packages.

Hence, this work developed a homomorphic encryption technique to secure cross-border transactions while protecting sensitive financial data. The transaction details and user identities are encrypted, the network ensured confidentiality and integrity during fund transfers. This enhanced security facilitated seamless and trustworthy cross-border payments, reducing the risk of fraud and unauthorized access to financial information.

2. METHOD

2.1. Literature survey

This section reviews the literature in the domain of financial applications using homomorphic encryption. This section mainly considers recent work happening with respect to homomorphic encryption techniques. The main focus is to identify gaps in the current literature with respect to applications of homomorphic encryption. The summary of literature survey is given in Table 1.

Table 1. Summary of literature survey

Source	Key issues	Suggested solution
Acar *et al.* [23]	Performance and efficiency challenges in FHE	To develop more efficient algorithms and hardware to enhance performance
Lauter *at al.* [24]	Feasibility and practicality of FHE in real-world applications	To implement algorithm and hardware advancements for better efficiency and accessibility
Ogburn *et al.* [25]	Viability and practical application of homomorphic encryption	To address theoretical and practical challenges to ensure effective real-world deployment
Shah *et al.* [26]	Efficiency of Paillier cryptosystem for encrypted image processing	To ptimize Paillier cryptosystem for better performance in image processing tasks
Iezzi [27]	Scalability and efficiency of homomorphic encryption in data science	To enhance scalability and efficiency through improved implementations and balancing data confidentiality with computational capabilities

Acar *et al.* [23] stated that the homomorphic encryption is a cryptographic approach that permits computations to be completed on encrypted information without decrypting it first, accordingly to make sure the statistics privateness and security at some point of the computational manner. The authors explore numerous homomorphic encryption schemes, focusing on their theoretical foundations and practical implementations. It highlights the improvements in absolutely fully homomorphic encryption (FHE), which helps arbitrary computation on ciphertexts, and discusses the demanding situations in performance and the performance that need to be addressed for broader adoption in real-global applications.

Lauter *et al.* [24] investigated the feasibility of the use of homomorphic encryption in realistic packages. It evaluates the computational and performance demanding situations associated with completely FHE and discusses capability optimizations and enhancements. The authors highlight advancements in algorithms and hardware that could make FHE greater efficient and accessible, thereby enhancing its practicality for stable facts processing in diverse industries.

Ogburn *et al.* [25] examined the viability and application of homomorphic encryption in safeguarding information. It delves into the theoretical underpinnings, diverse encryption schemes, and sensible implementations. Author highlighted the potential and the challenges of employing homomorphic encryption in real-world situations to ensure records privacy whilst making an allowance for computations on encrypted statistics.

Shah *et al.* [26] explored the usage of the Paillier cryptosystem to safely compute suggest values in encrypted picture processing. This method permits computations to be completed without delay on encrypted facts, maintaining privacy at the same time as allowing practical photograph processing tasks. The authors reveal how this method can be applied correctly, discussing each the theoretical foundations and sensible implementations.

Iezzi [27] provides a comprehensive overview of the ways a homomorphic encryption can be employed to make certain privateness in records technology applications. It discusses the theoretical aspects of homomorphic encryption, its sensible implementations, and the challenges faced in making this technology green and scalable for real-world data science obligations. The authors emphasizes the balance between maintaining statistics confidentiality and enabling meaningful computations on encrypted datasets.

2.2. Implementation

In this project, a secure data processing method is applied related to user authentication, homomorphic encryption, and database garage to ensure information privacy and safety. The working of proposed approach is explained in the subsequent paragraphs and architecture is shown in the Figure 1. Initially, a user interacts with the system, starting the method. The device authenticates the consumer through diverse authentication strategies which includes passwords, biometrics, or factor authentication, ensuring that most effective authorized customers. Upon a hit authentication, the person's records is encrypted using homomorphic encryption. This encryption technique lets in computations to be carried out on encrypted statistics, producing consequences that, while decrypted, fit those that might be obtained if the operations had been completed on the plaintext statistics. This guarantees that the information stays private even all through processing.

The encrypted statistics is then transmitted to a server, which acts as an middleman accountable for handling statistics processing duties. Importantly, because the records stays encrypted, the server can process it without accessing the actual content, appreciably improving safety. Subsequently, the server stores the encrypted information in MongoDB, a NoSQL database acknowledged for its capability to deal with large volumes of statistics correctly. MongoDB organizes the records into collections and documents, facilitating efficient storage and retrieval.

When data need to be accessed, the system determines how to build up and take care of the necessary facts, which may additionally contain aggregating records from one-of-a-kind resources or preparing it for unique operations. Mathematical operations are then executed on the encrypted data. Using homomorphic encryption, these operations may be achieved without decrypting the records, retaining the records's confidentiality and integrity.

At the last, machine evaluates the consequences of those operations in opposition to predefined threshold values to make selections. These threshold values assist to determine if specific situations are met or if positive actions have to be taken primarily based at the processed facts. This method guarantees a steady and privateness-preserving facts processing pipeline, from consumer authentication and records encryption to stable storage and computation.

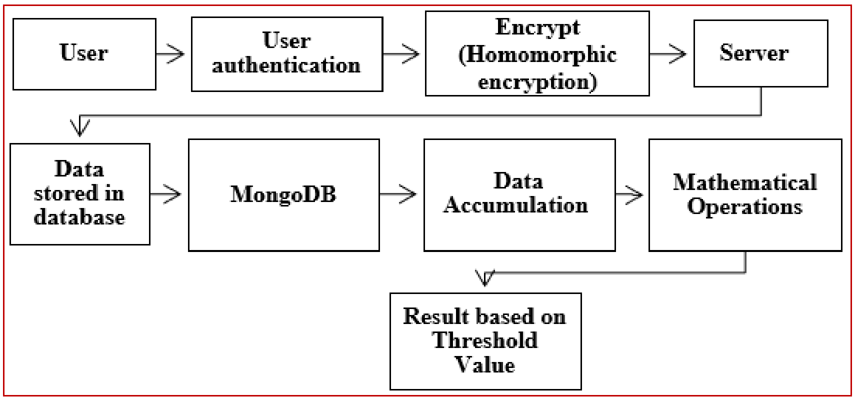

Figure 1. Architecture and process diagram

In this project, a secure data handling system is implemented using MongoDB for storage and encryption to ensure data privacy and security. As shown in Figure 2, the process begins with a user initiating a data upload from their device. Before the upload, the user need authentication through a secure authentication process to ensure only authorized individuals can proceed. Once data is authenticated, the data is uploaded to the server, where it is encrypted to maintain confidentiality. The encrypted data is then stored in MongoDB, it is organized into various tables for efficient management. When data access is required, the system retrieves the encrypted data from MongoDB and sends it to the user. At the user's end, the data is decrypted, ensuring only authorized users can view the plaintext information. The decrypted data, including any computed results, is then presented to the user. This method ensures end-to-end security, protecting the data from unauthorized access at all stages, from initial upload through storage to final retrieval and decryption. The method starts offevolved with the person importing information to the server. Before the information is stored at the server, it is encrypted using a mixture of keys and values. These encrypted facts are then saved in extraordinary tables within a MongoDB database on the server. When a person wants to get entry to their facts, they first need to go through a user authentication method. Once authenticated, the information is retrieved from MongoDB and decrypted at the consumer degree. This decrypted records is then computed and supplied to the consumer.

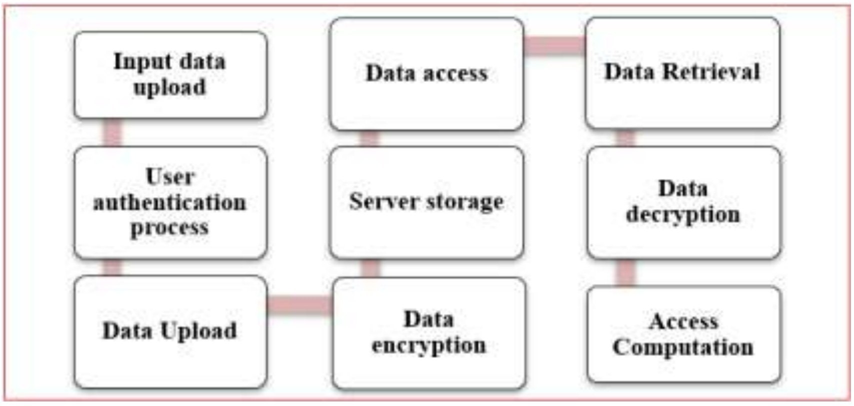

Figure 2. System flow diagram

3. RESULTS AND DISCUSSION

The key outcomes of this study are listed in this section. This work mainly improves system performance, provide secure data processing using homomorphic encryption and data storage on the MongoDB database. The financial application is secured by this work. The key outcomes are discussed below.

The proposed system developed abilities to perform computations on encrypted data without requiring decryption at any point, the confidentiality and integrity of financial information. This system mainly uses a combination of secure user authentication technique, encrypted data storage in MongoDB, and secure encrypted computations on the server side. The developed system implemented a cross-border transactions, where both user identities and transaction details were encrypted. The confidentiality is maintained on the network during fund transfers, it reduces the risks of fraud and unauthorized access of financial data. The system does encrypted computations such as interest rate calculations, risk assessments, and fraud detection on financial data without any leakage of sensitive information.

The implemented system gives better performance while performing financial transactions despite the complexity of homomorphic encryption. The system has little computational latency due to the encryption and decryption processes. These results are also aligned with the limitations of homomorphic encryption.

The homomorphic encryption-based approach ensured that sensitive financial data is remains encrypted during computations. This encryption significantly enhances data security by mitigating the risks of data breaches or unauthorized access. The system is resilient to common attacks targeting financial system, as the data remains unreadable even to the server processing the computations.

The MongoDB database is used for storage and retrieval of data which handles encrypted data. The MongoDB provides an efficient platform for organization and retrieval of encrypted financial data. The secure storage of encrypted data from unauthorized users protects sensitive financial information.

The user authentication system incorporates multi-factor authentication, provides an additional layer of security. This allows only authorized users to access the system. This technique makes the system more and enhances overall security. The results of this work make financial applications secure by applying homomorphic encryption. The system successfully does the encryption of financial data and performs computations.

The computational complexity of encrypted data leads to more processing time. To overcome this issue optimization techniques can be used in future research to enhance system efficiency. The management of encryption key is also a major challenge. In large transactions multiple keys need to be generated hence handling or loss of data is a challenging issue. The homomorphic encryption must follow data privacy regulations. There is lack of standards in the use of homomorphic encryption so there can be issue of interoperability while using this technique on the machines with varying architecture and data formats. The future research needs to focus on reducing computational overhead, efficient key management, and developing standard protocol for development of homomorphic encryption in financial encryption.

4. CONCLUSION

The application of homomorphic encryption in secure financial consultancy presents a promising avenue for enhancing data privacy and security in financial services. Allowing the computations on encrypted data without decryption, the homomorphic encryption ensures the confidentiality and integrity of sensitive financial information. Key findings underscore its potential to enable secure collaboration, uphold regulatory compliance, and foster trust between financial institutions and clients. Despite challenges such as computational overhead and key management complexity, homomorphic encryption offers significant benefits for safeguarding client data while facilitating advanced analytics and computations. In future, the regulatory adaptation, and industry collaboration will be crucial for realizing the full potential of homomorphic encryption in secure financial applications.

REFERENCES

[1] I. Damgård and M. Jurik, "A generalisation, a simplification and some applications of Paillier's probabilistic public-key system," in *ublic Key Cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC*, 2001, pp. 119–136, doi: 10.1007/3-540-44586-2_9.

[2] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 223–238.

[3] B. Chen and N. Zhao, "Fully homomorphic encryption application in cloud computing," in *2014 11th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2014*, 2014, pp. 471–474, doi: 10.1109/ICCWAMTIP.2014.7073452.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

[5] W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, "Accelerating fully homomorphic encryption using GPU," in *2012 IEEE Conference on High Performance Extreme Computing, HPEC 2012*, 2012, pp. 1–5, doi: 10.1109/HPEC.2012.6408660.

[6] L. Chen, H. Ben, and J. Huang, "An encryption depth optimization scheme for fully homomorphic encryption," in *Proceedings - 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2014*, 2014, pp. 137–141, doi: 10.1109/IIKI.2014.35.

[7] Y. Yang, S. Zhang, J. Yang, J. Li, and Z. Li, "Targeted fully homomorphic encryption based on a double decryption algorithm for polynomials," *Tsinghua Science and Technology*, vol. 19, no. 5, pp. 478–485, 2014, doi: 10.1109/TST.2014.6919824.

[8] M. Togan and C. Plesca, "Comparison-based computations over fully homomorphic encrypted data," in *2014 10th International Conference on Communications (COMM)*, May 2014, pp. 1–6, doi: 10.1109/ICComm.2014.6866760.

[9] S. M. Anggriane, S. M. Nasution, and F. Azmi, "Advanced e-voting system using Paillier homomorphic encryption algorithm," in *2016 International Conference on Informatics and Computing (ICIC)*, 2016, pp. 338–342, doi: 10.1109/IAC.2016.7905741.

[10] M. Nassar, A. Erradi, and Q. M. Malluhi, "Paillier's encryption: implementation and cloud applications," in *2015 International Conference on Applied Research in Computer Science and Engineering (ICAR)*, Oct. 2015, pp. 1–5, doi: 10.1109/ARCSE.2015.7338149.

[11] Y. Zhang, L. Zhuo, Y. Peng, and J. Zhang, "A secure image retrieval method based on homomorphic encryption for cloud computing," in *2014 19th International Conference on Digital Signal Processing*, Aug. 2014, vol. 2014-Janua, pp. 269–274, doi: 10.1109/ICDSP.2014.6900669.

[12] K. Shatilov, V. Boiko, S. Krendelev, D. Anisutina, and A. Sumaneev, "Solution for secure private data storage in a cloud," in *2014 Federated Conference on Computer Science and Information Systems, FedCSIS 2014*, Sep. 2014, pp. 885–889, doi: 10.15439/2014F43.

[13] C. Gentry, "A fully homomorphic encryption scheme," Stanford university, 2009.

[14] P. Bonsma, J. Schulz, and A. Wiese, "A constant factor approximation algorithm for unsplittable flow on paths," in *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, Oct. 2011, pp. 47–56, doi: 10.1109/FOCS.2011.10.

[15] S. Halevi and V. Shoup, "Algorithms in HElib," in *Advances in Cryptology--CRYPTO 2014: 34th Annual Cryptology Conference*, 2014, pp. 554–571, doi: 10.1007/978-3-662-44371-2_31.

[16] J. W. Bos, K. Lauter, J. Loftus, and M. Naehrig, "Improved security for a ring-based fully homomorphic encryption scheme," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, pp. 45–64, doi: 10.1007/978-3-642-45239-0_4.

[17] M. Kim and K. Lauter, "Private genome analysis through homomorphic encryption," *BMC Medical Informatics and Decision Making*, vol. 15, no. S5, p. S3, Dec. 2015, doi: 10.1186/1472-6947-15-S5-S3.

[18] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "Faster fully homomorphic encryption: bootstrapping in less than 0.1 seconds," in *Advances in Cryptology--ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security*, 2016, pp. 3–33, doi: 10.1007/978-3-662-53887-6_1.

[19] R. Palle and A. Punitha, "Privacy-preserving homomorphic encryption schemes for machine learning in the cloud," *ESP Journal of Engineering & Technology Advancements*, vol. 1, no. 2, pp. 21–33, 2021, doi: 10.56472/25832646/JETA-V1I2P106.

[20] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory*, vol. 6, no. 3, 2014, doi: 10.1145/2633600.

[21] A. Costache and N. P. Smart, "Which ring based somewhat homomorphic encryption scheme is best?," in *Topics in Cryptology-CT-RSA 2016: The Cryptographers' Track at the RSA Conference 2016*, 2016, pp. 325–340, doi: 10.1007/978-3-319-29485-8_19.

[22] M. Wu, X. Zhao, and W. Song, "Bootstrapping optimization for fully homomorphic encryption schemes," *Research Square Preprint*, Apr. 2024, doi: 10.21203/rs.3.rs-4194403/v1.

[23] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–35, Jul. 2019, doi: 10.1145/3214303.

[24] K. Lauter, M. Naehrig, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2011, pp. 113–124, doi: 10.1145/2046660.2046682.

[25] M. Ogburn, C. Turner, and P. Dahal, "Homomorphic encryption," *Procedia Computer Science*, vol. 20, pp. 502–509, 2013.

[26] M. Shah, W. Zhang, H. Hu, and N. Yu, “Paillier cryptosystem based mean value computation for encrypted domain image processing operations,” *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 15, no. 3, pp. 1–21, 2019, doi: 10.1145/3325194.

[27] M. Iezzi, “Practical privacy-preserving data science with homomorphic encryption: an overview,” *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*. pp. 3979–3988, 2020, doi: 10.1109/BigData50022.2020.9377989.

BIOGRAPHIES OF AUTHORS

Dr. Vijaykumar Bidve is an associate professor at Symbiosis Skills and Professional University, Kiwale, Pune, Maharashtra, India. He holds a Ph.D. degree in Computer Science and Engineering with specialization in Software Engineering. His research areas are software engineering and machine learning. He has published 11 patents. He has published more than 50+ research articles in national and international journals. He is a life member of ISTE. He is working as an expert on various subjects. Also, he has worked as a reviewer for various conferences and journals. He can be contacted at email: vijay.bidve@gmail.com.

Dr. Aruna Pavate is working as associate professor Thakur College of Engineering and Technology Mumbai Maharashtra India. Senior research fellow, University of Economy and Pedagogy, Department of Scientific Research, Innovation and Training of Scientific and Pedagogical Staff, University of Economics and Pedagogy, Karshi, Uzbekistan. Her research interests include machine learning and security, data mining, data science, and cyber security. She is a member of various professional bodies including ISTE, IAENG, AICTSD, Insc and IEEE and editor for ASMS, IIP. She has worked as program chair for many the conferences and for journals such as JEET, journal of experimental and theoretical artificial intelligence, expert systems with applications, Applied artificial intelligence, Ad-hoc reviewer for International Journal of Ambient Computing and Intelligence. She has published more than 50 articles in various journals and conferences. She can be contacted at email: arunaapavate@gmail.com.

Mr. Rahul Raut is working as assistant professor at the School of CSIT at Symbiosis Skill and Professional University, Kiwale, Pune, Maharashtra. He has completed his M.Tech. degree from S.G.B. Amravati University, MS, India. He is currently a research fellow with S.G.B. Amravati University, Maharashtra, India. He has published two books with reputed publisher, one book chapter and over 15 conference and journal papers. His research interests broadly include vehicular Ad-hoc network, mobile Ad-hoc network, signal processing for communication, machine learning, and neural network. He can be contacted at email: mr.rahulraut@gmail.com.

Dr. Shailesh Kediya is associate professor at Symbiosis Skills and Professional University, Kiwale, Pune, Maharashtra, India. He holds a Ph.D. degree in Logistics Management. His research areas are innovative and disruptive technologies, business management. He has awarded with 3 international patents and 4 national patents, awarded with 14 copyright and authored 11 books. He has published more than 50 research articles in national and international journals. He is a member of IEEE, SEBI, and NISM. He is working as an expert for various subjects. Also, he has been editor of four international journals and worked as a reviewer for various conferences and journals. He can be contacted at email: kediya.shailesh@gmail.com.

Dr. Pakiriswamy Sarasu is professor at Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India. She holds a Ph.D. degree in Computer Science and Engineering. She did her masters in Embedded Systems Technology and Bachelors in Computer Science Engineering. Her research areas include chaotic systems, cryptography, and autonomous vehicle. She played a major role in creating innovation entrepreneurial ecosystem and more than 120 startups are created under her guidance and mentorship. One patent is granted for her as one of the inventors. She can be contacted at email: sarasujivat@gmail.com.

Dr. Koteswara Rao Anne is working as Dean, Mukesh Patel School of Technology Management and Engineering, NMIMS, Mumbai. He is a distinguished researcher in information technology and engineering education with a doctorate from the University of Klagenfurt, Austria. He has published over 15 papers on problem-based and challenge-based learning pedagogies. In social signal processing, he has authored 45 papers and a book on acoustic modeling for emotion recognition. His work has resulted in seven Indian patents. He has supervised five Ph.D. students and significantly contributed to India's National Board of Accreditation becoming a Washington Accord signatory. He is active in international education communities and serves on various academic boards across India. He can be contacted at email: raoanne@gmail.com.

Dr. Aryani Gangadhara is associate professor at Department of F.Y. B.Tech., D. Y. Patil College of Engineering, Pune, India. A passionate teacher who believes in learning interdisciplinary skills with the basic foundation of Mathematics and Statistics. She is also guest faculty at BITS-Pilani, WILP division. She holds a Ph.D. degree in Mathematics with specialization in Hyperlattice Theory. She has qualified SET and GATE. Her research areas are hyper lattice theory, time series analysis, machine learning, and deep learning. She has published 11 research articles in national and international journals. She is author of Book Discrete Mathematics, PTU. She is a life member of Indian Mathematical Society (IMS). She can be contacted at email: aryanimaths@gmail.com.

Dr. Ashfaq Shaikh is working as assistant professor at M. H. Saboo Siddik College of Engineering, Byculla, Mumbai, India with 23 year of teaching experience. He is Ph.D. Computer Engineering with a specialization in big data analytics, machine learning, recommendation system, information, and cyber security. His passion for teaching and innovation contribution resulted in winning several awards and recognition such as Mastek Deep Blue Winner in 2017, AICTE Best Team Award in Smart India Hackathon in 2018, and Best Faculty Award in year 2021. He can be contacted at email: ashfaq.mhss@gmail.com.