Cloud Data Security: Advanced Cryptography Algorithms

Rambabu Nalagandla and Ojasvi Pattanaik

August 27, 2023

Cloud Data Security: Advanced Cryptography Algorithms

1stRambabu Nalagandla

Program Manager,IT Risk and Control Leader

Email:rams.devops36@gmail.com

2rd Ojasvi Pattanaik
Btech, Computer Science and Engineering, Vignan institute of management and technology for women, Ghatkesar, JNTU,Hyderabad

Email:ojasvipattanaik22@gmail.com,

***Abstract*—As enterprises increasingly store and handle sensitive data on the cloud, cloud data security is a major problem. Advanced cryptography techniques help secure this critical data. This abstract discusses how sophisticated encryption methods protect cloud data. Cloud services are in significant demand, necessitating better data security. It stresses cloud risks such data interception, illegal access, and insider attacks. Advanced encryption techniques protect sensitive data. The abstract then describes sophisticated encryption techniques' data secrecy, integrity, and authenticity. Symmetric and asymmetric encryption schemes are examined for cloud data security at rest and in transit. The abstract emphasizes key management in cryptography techniques to protect encrypted data. Key creation, distribution, storage, and revocation are examined, emphasizing their importance in protecting cloud-stored data. In cloud computing, cryptography techniques must be scalable and efficient. It discusses homomorphic encryption, secure multi-party computing, and zero-knowledge proofs, which allow safe computation and data processing while protecting privacy. The abstract also recognizes cryptography algorithm innovation to combat new threats. It discusses post-quantum cryptography strategies to protect present encryption methods against quantum computer advances. Advanced cryptography methods are crucial to cloud data security. These algorithms underpin safe cloud computing with secrecy, integrity, authenticity, and scalability. As cloud use rises, enterprises must prioritize powerful encryption algorithms to secure sensitive data and defend against new cyber threats.**

Keywords—Advanced cryptography techniques, Cloud Computing, FHE, MPC, PHE, GDPR, ECC

I. INTRODUCTION

Today's digital world relies on cloud computing to store and retrieve vital data, making cloud data security a major issue. Advanced encryption techniques protect cloud-stored sensitive data. These algorithms safeguard data using advanced mathematical methods. These cutting-edge cryptography techniques reduce data access, interception, and manipulation threats [1]. Cloud data security uses homomorphic encryption. This breakthrough method computes encrypted data without decryption. Homomorphic encryption protects sensitive data during computations in the cloud [2].

Elliptic Curve Cryptography (ECC) provides more security than public key encryption. Elliptic curves enable efficient and robust encryption, making ECC ideal for resource-constrained applications like cloud computing. ECC is a good solution for cloud data security and performance since it provides equal protection with lower key lengths [3]. Multi-Party Computation (MPC) uses advanced cryptographic techniques to safeguard cloud data analysis and processing without forcing data owners to provide sensitive information. Decentralized computing improves cloud-based systems' trust and secrecy [4].

Traditional encryption solutions may not defend against clever attackers and increasing computer power. Advanced algorithms withstand brute-force assaults, cryptographic flaws, and other malevolent methods [5]. ECC is ideal for resource-constrained cloud computing systems that must optimize speed without sacrificing data safety [6]. MPC lets several parties compute on their private data while protecting individual inputs. MPC uses powerful cryptographic techniques to safeguard cloud data analysis and processing without disclosing sensitive information [7]. Homomorphic encryption, elliptic curve cryptography, and safe multi-party computation may improve cloud computing security, privacy, and trust [8].

Symmetric and asymmetric encryption systems need decryption before computing, putting data at risk. Homomorphic encryption solves this difficulty by enabling calculations on encrypted data without decryption and re-encryption [9]. A partly homomorphic encryption technique may enable just addition or multiplication on encrypted data. This constraint permits calculations inside a mathematical domain while protecting data. It is unsuitable for general-purpose calculations [10]. FHE is the most powerful and flexible homomorphic encryption. It permits unlimited calculations on encrypted data [11].

Homomorphic encryption is slower and more resource-intensive than typical encryption techniques due to computational complexity. Homomorphic encryption performance depends on data size and processing complexity [12]. Homomorphic encryption is used in safe compute outsourcing, collaborative machine learning, and privacy-enhanced data exchange. Homomorphic encryption, a ground breaking cryptographic method, allows calculations on encrypted data while guaranteeing data secrecy. Homomorphic encryption may secure and protect cloud computing and other computations using sophisticated mathematical procedures [13]. Various homomorphic encryption algorithms have various functionality and processing capabilities. Partially homomorphic encryption techniques allow addition and multiplication calculations on encrypted data [14].

Encryption and decryption need extensive processing resources due to complicated mathematical calculations [15]. Homomorphic encryption has several non-cloud uses. Homomorphic encryption is useful beyond safe data outsourcing and privacy-preserving data analytics. It allows private machine learning collaborations where several parties may train models on their encrypted data without disclosing critical information. Homomorphic encryption allows private data exchange [16]. Despite computational obstacles, homomorphic encryption research is improving its efficiency and practicality, broadening its applications, and unleashing its promise for safe and privacy-preserving data processing [17].

Complex mathematical procedures and techniques secure encrypted data during computation. Homomorphic encryption protects data against illegal access and disclosure [18]. Partially homomorphic encryption techniques offer limited data operations like addition and multiplication. These techniques are helpful for data privacy-preserving calculations inside a mathematical domain [19]. Complex mathematical procedures alter encrypted data while maintaining secrecy during encryption and decryption [20]. Holomorphic encryption uses complex mathematics like lattice-based cryptography or rings or groups [21]. These mathematical underpinnings prevent encrypted data computations from revealing plaintext. Methods and Materials [22]

Fully Homomorphic Encryption (FHE)

Fully Homomorphic Encryption (FHE) is a sophisticated cryptographic method that permits arbitrary calculations on encrypted data without decryption. FHE allows calculations on encrypted data without decrypting it, retaining secrecy. FHE uses complicated mathematical procedures to secure encrypted data during computation. FHE's major goal is to allow safe and privacy-preserving computations on sensitive data even in untrusted contexts like cloud servers. After introducing FHE in the late 1970s, researchers needed decades to build practical and efficient FHE methods. Designing encryption techniques that permit arbitrary computations without compromising security or performance is the core problem of FHE.

FHE computes on encrypted data, called ciphertexts. FHE schemes encrypt data with a particular key and allow calculations without decryption. The authorized person with the decryption key may decrypt these calculations. FHE techniques use difficult mathematical ideas like lattice-based encryption or rings or groups. These mathematical underpinnings allow encrypted data calculations without disclosing the plaintext.

PHE and FHE are the primary types of FHE systems. PHE algorithms may compute addition and multiplication on encrypted data. PHE schemes have uses, but they have computing limits. FHE techniques allow any calculation on encrypted data. FHE can calculate any plaintext function on encrypted data. FHE involves solving efficiency, scalability, and security issues, making research difficult.

FHE faces processing cost while computing on encrypted data. FHE techniques are more computationally demanding than typical encryption methods, which may impede processing and raise resource needs. FHE techniques are being optimized using faster algorithms. Key management and system security are major FHE challenges. FHE calculations use several encryption and decryption keys. These keys must be kept secret and secure to protect encrypted data and the system.

FHE is promising in several areas despite its obstacles. Cloud computing, data sharing, and collaborative analysis need safe, privacy-preserving processing. In healthcare, banking, and machine learning, FHE processes sensitive data while protecting privacy. Fully Homomorphic Encryption (FHE) is a sophisticated cryptographic method that permits arbitrary calculations on encrypted data without decryption. It allows safe and privacy-preserving computing on sensitive data and might change data security in several fields. Research and development are aimed at addressing efficiency and security issues and maximizing FHE's potential.

FHE research is constantly addressing issues and constraints. FHE efficiency and practicality are being improved by new algorithms, optimizations, and hardware technologies. These initiatives seek to make FHE more accessible, efficient, and scalable, allowing its inclusion into applications and areas that demand safe and privacy-preserving calculations. FHE facilitates encrypted data calculations. FHE allows arbitrary calculations on encrypted data without decryption, allowing privacy-preserving computation and safe data processing. FHE research and development may improve data security and privacy in many applications, despite computational complexity and key management issues.

FHE is a cutting-edge cryptographic method that has revolutionized data security and privacy. FHE enables calculations directly on encrypted data, protecting sensitive data throughout the process. Traditional encryption techniques need decryption before computations. Cryptography research and invention led to FHE. Researchers have made great progress toward FHE, which allows arbitrary computations on encrypted data, by building on partly homomorphic encryption techniques. This invention has enabled safe data processing, particularly in data-sensitive situations like cloud computing and outsourced compute.

FHE addresses data leaks and privacy breaches during data processing and analysis. FHE keeps encrypted data encrypted during computation, preventing even the calculation party from accessing the plaintext. In cloud computing, data is outsourced to third-party computers, allowing safe and privacy-preserving calculations on sensitive data. FHE is also driven by the requirement for privacy-preserving collaborative data analysis and sharing. FHE lets parties compute on encrypted data without data exchange or decryption. In healthcare, finance, and research, companies and people must interact and obtain insights from integrated data without sacrificing privacy.

PHE (Partially Homomorphic Encryption)

Partially Homomorphic Encryption (PHE) is a cryptographic system that improves data privacy while allowing certain calculations on encrypted data. PHE balances FHE's security with symmetric and asymmetric encryption techniques' simplicity and efficiency. In privacy-sensitive situations, it computes encrypted data without decryption. PHE protects sensitive data while allowing calculations on it. Symmetric and asymmetric encryption techniques prevent calculations on encrypted material without decryption. PHE, on the other hand, allows specialized activities on encrypted data without compromising secrecy.

PHE uses homomorphic encryption scheme-preserving mathematical processes to deliver this feature. PHE provides encrypted data addition and multiplication, but not arbitrary computations like FHE. This allows calculations on encrypted values without compromising data privacy. PHE's adaptability makes it versatile. In cloud computing, where sensitive data is typically outsourced to faraway servers, PHE permits calculations on encrypted data, avoiding security problems. This is especially useful when privacy or data protection laws restrict raw data exchange or processing.

PHE can secure decentralized computation. PHE lets many participants cooperatively calculate a result using encrypted data. PHE lets parties compute together while keeping their inputs secret, protecting sensitive data. Secure data analysis and machine learning use PHE. Organizations and researchers must undertake statistical calculations, aggregations, and predictive modeling on sensitive data without compromising privacy. PHE computes on encrypted data to protect sensitive information from unwanted access. PHE is easier than completely homomorphic encryption. PHE schemes are simpler and less computationally intensive than fully homomorphic ones. This makes PHE more applicable in real-world applications where efficiency and simplicity matter.

PHE helps solve the data privacy-computation conflict. Data owners are wary of sharing sensitive information owing to worries about illegal access, data breaches, and privacy violations. PHE allows specialized calculations on encrypted data, balancing privacy and functionality.

Multi-Party Computation (MPC)

Multi-Party Computation (MPC) is a cryptographic mechanism that lets many people compute on secret data without disclosing inputs. MPC lets people cooperate and get relevant results without exposing their raw data, maintaining privacy and secrecy. Secure computing, which tries to compute sensitive data while protecting privacy, inspired MPC. A trustworthy third party facilitated safe computing in traditional methods. MPC lets players compute directly without a trusted third party.

MPC protocols prevent parties from learning about one other's secret inputs except from the end output. Encryption, secret sharing, and secure function evaluation accomplish this. Secret sharing, where each person separates their private contribution into many shares and distributes them, is the core of MPC. These shares are carefully designed to conceal the actual input while enabling proper calculation. The participants then calculate shares of the output using their shares of the inputs, ensuring that the intermediate outcomes do not reveal any private input information.

MPC protocols safeguard calculations through cryptographic primitives and algorithms. Cryptographic hash functions, symmetric and asymmetric encryption techniques, digital signatures, and commitment mechanisms. MPC protects computation privacy and integrity even with malevolent actors by using cryptographic methods. MPC is used to collaboratively analyze sensitive data. Multiple hospitals may desire to collectively analyze patient data to detect trends and patterns without compromising patient details. MPC allows hospitals to provide encrypted data for privacy-preserving analysis.

Secure auctions, when several bidders desire to participate without exposing their bids, use MPC. MPC allows the auctioneer to calculate the winning offer without knowing any bids, assuring a fair and private auction. MPC is also useful in GDPR-regulated environments. MPC lets organizations share and analyze data while complying with privacy laws. Data-driven insights and decision-making safeguard privacy.

MPC guarantees anonymity but has drawbacks. Cryptographic processes in secure computing add computational cost. Complex MPC procedures increase computational costs and processing speeds. MPC techniques are being optimized for real-world use by researchers. MPC is a cryptographic system that lets several participants compute privately on their private data. MPC uses cryptography and secure function evaluation to safeguard analysis, collaboration, and decision-making without disclosing inputs. MPC is a useful tool for privacy-preserving data processing in healthcare, banking, and data privacy compliance, but research is continuing to increase its efficiency and applicability.

II. Results and Discussion

Figure 1 shows FHE use by industry from 2018 to 2022. In 2018, Manufacturing used 100 units of FHE and IT used 200. Healthcare and Finance used 100 units apiece. 2018 consumed 600 units.

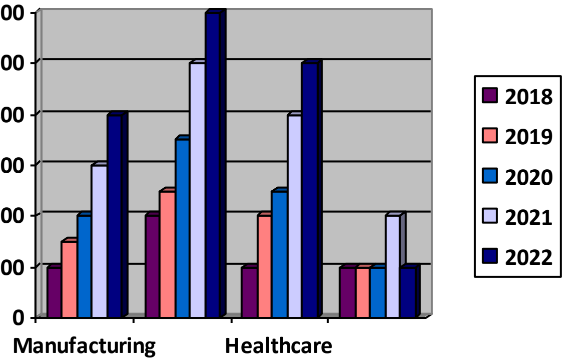

Fig. 1. Representing the year-wise consumption of Fully Homomorphic Encryption (FHE) by various industry areas from 2018 to 2022

In 2019, all industries consumed more. Manufacturing utilized 150 units, IT 250, Healthcare 200, and Finance 100. 2019 consumed 700 units. Consumption rose in 2020. Manufacturing, IT, Healthcare, and Finance consumed 200, 350, 250, and 100 units, respectively. 2020 used 900 units. FHE use increased in 2021. Manufacturing used 300 units, IT 500, and Healthcare 400. Finance did not utilize FHE units this year. 2021 used 1200 units. Consumption rose in 2022. Manufacturing used 400 units, IT 600, Healthcare 500, and Finance 100. 2022 used 1600 units.

Figure 2 shows industry-specific MPC usage from 2018 to 2022. Manufacturing used 50 MPC units in 2018, while IT used 100. Healthcare used 75 units and Finance 25. 2018 consumed 250 units. In 2019, all industries consumed more. Manufacturing used 75 units, IT 150, Healthcare 100, and Finance 50. 2019 consumed 375 units. Consumption rose in

2020. Manufacturing utilized 100 units, IT 200, Healthcare 125, and Finance 75. 2020 used 500 units. MPC consumption increased in 2021. Manufacturing used 150 units, IT 250, Healthcare 175, and Finance 100. 2021 used 675 units. Finally, consumption rose in 2022. Manufacturing used 200 units, IT 300, Healthcare 200, and Finance 125. 2022 used 825 units. This statistic shows the year-by-year consumption of Multi-Party Computation (MPC) by different industries, showing its growing popularity and use. Data sensitivity, legal restrictions, industry-specific use cases, and industry knowledge of privacy-preserving technologies like MPC may affect industry use.

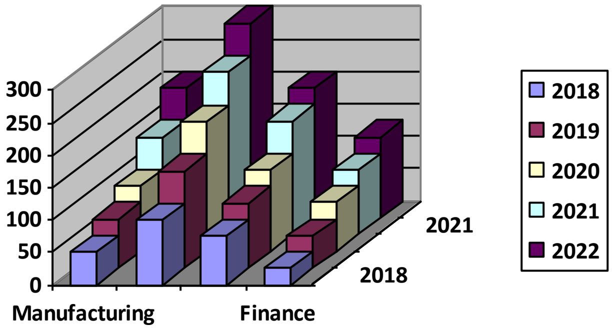

Fig. 2. Representing the year-wise consumption of Multi-Party Computation (MPC) by various industry areas from 2018 to 2022

Figure 3 shows industrial utilization of Partially Homomorphic Encryption (PHE) from 2018 to 2022.

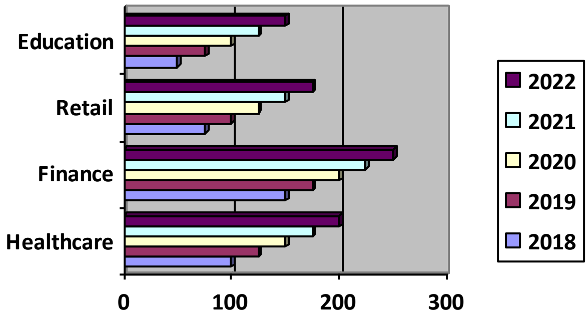

Fig. 3. Representing the year-wise consumption of Partially Homomorphic Encryption (PHE) by various industry areas from 2018 to 2022

Healthcare used 100 PHE units in 2018, while Finance used 150. Retail used 75 units and Education 50. 2018 consumed 375 units. In 2019, all industries consumed more. Finance used 175 units, Healthcare 125, Retail 100, and Education 75. 2019 consumed 475 units. Consumption rose in 2020. Healthcare used 150 units, Finance 200, Retail 125, and Education 100. 2020 used 575 units. PHE consumption increased in 2021. Healthcare used 175 units, Finance 225, Retail 150, and Education 125. 2021 used 675 units. Finally, consumption rose in 2022. Healthcare used 200 units, Finance 250, Retail 175, and Education 150. 2022 used 775 units. This data shows how industrial sectors are adopting and using Partially Homomorphic Encryption (PHE) year-by-year. Specific data processing needs, privacy concerns, regulatory compliance, or industry-specific use cases where PHE is employed to secure calculations while protecting data secrecy may affect industry utilization. Table 1 summarizes MPC components, characteristics, and applications. MPC protects privacy, enables safe calculations, and builds trust among numerous parties.

TABLE I. A BREAKDOWN OF THE KEY COMPONENTS AND FEATURES OF MULTI-PARTY COMPUTATION (MPC)

Component/Feature	Description
Participants	Many parties or organizations that calculate together while protecting their private inputs. Everyone contributes to the computation.
Security	Maintains participant privacy throughout calculation. Cryptographic methods prohibit MPC participants from knowing each other's inputs.
Trust	MPC does not need a trusted third party or central authority. Distributed computations provide fairness, transparency, and participant control over inputs.
Privacy-Preserving Computation	MPC computes private inputs securely. Cryptographic protocols compute encrypted data without disclosing inputs.
Functionality	MPC provides arithmetic, logical, and complicated algorithms. MPC protocol and cryptographic primitives determine supported calculations.
Security Guarantees	MPC protocols safeguard private inputs, prevent collusion attacks, and prevent information leaking. Established cryptographic assumptions and proving methods underpin these promises.
Efficiency	MPC protocol efficiency matters. Secure calculations' computing cost depends on operation complexity, participant number, and cryptographic primitives. Research optimizes MPC techniques for efficiency.
Real-World Applications	Safe data sharing, collaborative analytics, privacy-preserving machine learning, voting systems, and multiparty discussions employ MPC. It protects private data by calculating outputs without divulging inputs.

Partially Homomorphic Encryption (PHE) components, characteristics, and concerns are summarized in Table 2. PHE is privacy-preserving, practical, and limited compared to Fully Homomorphic Encryption (FHE). The table shows significant use cases and concerns for applying PHE in real-world applications. Table 3 summarizes FHE's key components, characteristics, and concerns. It demonstrates FHE's tremendous homomorphic characteristics, ability to execute arbitrary calculations on encrypted data, and computational complexity. The table highlights FHE optimization difficulties and active research. Finally, it discusses FHE use cases and implementation issues.

TABLE II. PROVIDING A BREAKDOWN OF THE KEY COMPONENTS AND FEATURES OF PARTIALLY HOMOMORPHIC ENCRYPTION (PHE)

Component/Feature	Description
Homomorphic Propert	Homomorphic characteristics of PHE systems enable calculations on encrypted data without decryption. PHE allows encrypted value addition and multiplication, unlike Fully Homomorphic Encryption (FHE).

Privacy Preservation	PHE computes encrypted data to protect sensitive data. Only the encrypted data is shown. This avoids data leaks and unwanted access.
Selective Computation	PHE lets encrypted data be computed, balancing privacy and usefulness. PHE offers useful actions on encrypted values, making it ideal for many applications.
Use Cases	Cloud computing, decentralized collaborations, safe data analysis, and privacy-preserving machine learning use PHE. Secure computations on encrypted data provide insights and collaborative computations while protecting sensitive data.
Computational Limitations	PHE lacks FHE's advantages. PHE supports just addition and multiplication. PHE may not be suitable for complex procedures or iterative processes.
Data Privacy Regulations	PHE lets enterprises compute on encrypted data while complying with privacy standards. Data privacy-sensitive companies need this capability.
Implementation Considerations	Implementing PHE safely involves cryptography and system design knowledge. To guarantee PHE dependability, key management, secure communication methods, and system design should be carefully studied.

TABLE III. A BREAKDOWN OF THE KEY COMPONENTS AND FEATURES OF FULLY HOMOMORPHIC ENCRYPTION (FHE)

Component/Feature	**Description**
Homomorphic Properties	FHE systems' homomorphic features enable arbitrary calculations on encrypted material without decryption. FHE allows encrypted value addition and multiplication, allowing many calculations.
Privacy Preservation	FHE protects sensitive data by computing on encrypted data without disclosing the underlying information. Only the encrypted results are retrieved, protecting sensitive data.
Arbitrary Computations	FHE uses encrypted data to calculate. It conducts complicated Boolean circuits or machine learning algorithms on encrypted data, offering important functionality while securing data.
Circuit Complexity	FHE requires more processing than partly homomorphic encryption. FHE requires more computer resources and may take longer to compute encrypted data.
Current Research Efforts	Optimized FHE systems minimize computational cost and efficiency. Noise reduction, bootstrapping, and improved encryption algorithms make FHE practical for real-world applications.
Use Cases	Secure cloud computing, privacy-preserving machine learning, data sharing, and decentralized collaborations need FHE. Secure calculations on encrypted data protect sensitive information.
Implementation Challenges	Cryptography, system design, and computing efficiency skills are needed to safely implement FHE. A robust FHE implementation requires key management, secure communication routes, and efficient computation protocols.

III. CONCLUSION

Advanced encryption techniques safeguard cloud data. Cloud service demand and vulnerabilities need comprehensive protection. Cryptography algorithms protect sensitive data. Data secrecy, integrity, and authenticity make modern cryptography methods essential for cloud data security. Symmetric and asymmetric algorithms safeguard cloud data at rest and in transit. Encrypted data protection requires good key management. Cloud cryptography techniques must be scalable and efficient. Homomorphic encryption, safe multi-party computing, and zero-knowledge proofs provide private computation and data processing. Emerging risks need encryption algorithm evolution. Post-quantum cryptography methods are being developed to fight quantum computer advances that potentially weaken encryption. Organizations must prioritize sophisticated cryptography techniques to secure cloud data. These algorithms secure sensitive data, decrease cloud risks, and comply with data protection standards. Cloud data security requires modern cryptography techniques. Confidentiality, integrity, authenticity, scalability, and privacy-preserving calculations make them essential for cloud data security. As cloud services become more popular, enterprises must embrace and modify these complex algorithms to defend against emerging cyberthreats.

REFERENCES

[1] AE Adeniyi, KM Abiodun, JB Awotunde, M Olagunju, OS Ojo, and NP Edet, “Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach,” Multimedia Tools and Applications, vol. 13, pp. 1–5, 2023.

[2] Y Alemami, AM Al-Ghonmein, KG Al-Moghrabi, and MA Mohamed, “Cloud data security and various cryptographic algorithms,” International Journal of Electrical and Computer Engineering, vol. 13, no. 2, pp. 1–13, 2023.

[3] UI Erondu, EO Asani, MO Arowolo, AK Tyagi, and N Adebayo, “An Encryption and Decryption Model for Data Security Using Vigenere With Advanced Encryption Standard,” In Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services, pp. 141–159, 2023.

[4] AA Jabbar, and WS Bhaya, “Security of private cloud using machine learning and cryptography,” Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, pp. 561–569, 2023.

[5] KN Gottipati, N Peddisetty, S. Pothireddy, G Botta, P Yellamma, and G Swain, “A Study on Data Security and Privacy Issues in Cloud Computing,” Third International Conference on Artificial Intelligence and Smart Energy, pp. 451–458, 2023.

[6] AK Jaithunbi, S Sabena, and L Sairamesh, “Preservation of Data Integrity in Public Cloud Using Enhanced Vigenere Cipher Based Obfuscation,” Wireless Personal Communications, vol. 129, no.1, pp. 271–284, 2023.

[7] M Jalasri, and L Lakshmanan, “Managing data security in fog computing in IoT devices using noise framework encryption with power probabilistic clustering algorithm,” Cluster Computing, vol. 26, no. 1, pp. 823–836, 2023.

[8] AR Khan, and LK Alnwihel, “Brief Review on Cloud Computing Authentication Frameworks,” Engineering, Technology and Applied Science Research, vol. 13, no. 1, pp. 9997–10 004, 2023.

[9] Y Alemami, MA Mohamed, and S Atiewi, “Advanced approach for encryption using advanced encryption standard with chaotic map,” International Journal of Electrical and Computer Engineering, vol. 13, no. 2, pp. 1708–1723, 2023.

[10] S Soni, and P Gupta, “Analysis of Security of Cloud with Encryption by Utilizing Symmetric and Asymmetric Algorithm,” International Journal of Research Publication and Reviews, vol. 4, no. 1, pp. 270–278, 2023.

[11] AD Stefan, IP Anghel, and E Simion, “Quantum-Safe Protocols and Application in Data Security of Medical Records,” Cryptology ePrint Archive, pp. 1-14,2023.

[12] R Singh, and RK Pateriya, “Data Clustering Approach on the Basis of Data Sensitivity for Implementation of Secure Cloud Computing Environment,” In Machine Learning, Image Processing in Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND, pp. 715–724, 2021.

[13] NM Reddy, G Ramesh, SB Kasturi, D Sharmila, G Gopichand, and LT Robinson, “Secure data storage and retrieval system using hybridization of orthogonal knowledge swarm optimization and oblique cryptography algorithm in cloud,” Applied Nanoscience, vol. 13, no.3, pp. 2449–2461, 2023.

[14] UR Saxena, and T Alam, “Role-based access using partial homomorphic encryption for securing cloud data,” International Journal of System Assurance Engineering and Management, vol. 30, pp. 1–7, 2023.

[15] V Terziyan, D Malyk, M Golovianko, and V Branytskyi, “Encryption and Generation of Images for Privacy-Preserving Machine Learning in Smart Manufacturing,” Procedia Computer Science, vol. 217, pp. 91–101, 2023.

[16] TL Liao, CY Peng, and YY Hou, “Application of multi‐party computation and error correction with image enhancement and convolution neural networks based on cloud computing,” IET Image Processing, vol. 17, no. 6, pp. 1931–1950, 2023.

[17] Z Man, J Li, X Di, R Zhang, X Li, and X Sun, “Research on cloud data encryption algorithm based on bidirectional activation neural network,” Information Sciences, vol. 622, pp. 629–651, 2023.

[18] J Kotti, RR Chundru, J Sudhakar, and B Sreenidhi, “Aes Based Blood Bank System Using Cloud Techniques,” Journal of Pharmaceutical Negative Results, pp. 1070–1077, 2023.

[19] P Kuppuswamy, SQ Al, R John, M Haseebuddin, and AA Meeran, “A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm,” Bulletin of Electrical Engineering and Informatics, vol. 12, no. 2, pp. 1148–1158, 2023.

[20] AA Fairosebanu, and AC Jebaseeli, “Data security in cloud environment using cryptographic mechanism,” Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, pp. 462–471, 2023.

[21] B. Pattanaik, S. S. Kumari, K. Kumar C, M. Pattnaik, S. I. Ali and M. Kumarasamy, "An Innovation of Algebric Mathamatical Based Statistical Analysis Model for Complex Number Theory," 2023 International Conference on Disruptive Technologies (ICDT), Greater Noida, India, doi: 10.1109/ICDT57929.2023.10151169., [1] pp.94-99, 2023.

[22] R. Jain, Y. Bekuma, B. Pattanaik, A. Assebe and T. Bayisa, "Design of a Smart Wireless Home Automation System using Fusion of IoT and Machine Learning over Cloud Environment," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, doi: 10.1109/ICIEM54221.2022.9853116, pp. 840-847, 2022.