RESEARCH PAPER

Advanced Cloud Security and Privacy Preservation for Healthcare, Medical, and Drug Technology Data through Integration of Machine Learning and Cryptography

Chandra Mouli Darapaneni[1], Cmak Zeelan Basha[2], D. Deepthi[3], Gaddam Mounika[4], K. Thrilochana[5]

[1] Department of Civil Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
[2] Assistant Professor, Department of CSE, KLEF, Vaddeswaram, Guntur, AP
[3,4] Assistant Professor, R.V.R. & J.C College of Engineering, Guntur, AP
[5] Assistant Professor, Vasireddy Venkatadri Institute of Technology University, Namburu, Guntur

Received: 2nd Mar, 2026 | **Revised:** 14th Mar, 2026 | **Accepted:** 4th Apr, 2026 | **Available Online:** 20th Apr, 2026

ABSTRACT

In modern technological landscapes, private cloud security is of paramount concern due to the ever-increasing volume and complexity of cyber threats. This research article explores the integration of machine learning and cryptography as a means to enhance security within private cloud environments. This study aims to mitigate vulnerabilities that may compromise data integrity, confidentiality, and availability in private cloud infrastructures by using machine learning algorithms and strong cryptography. By detecting anomalous cloud patterns and behaviors, machine learning algorithms enable proactive threat detection. Machine learning models can distinguish normal network activity from malicious incursions by analyzing large datasets, improving early threat detection and response. By using cryptographic protocols like homomorphic encryption and multi-party computation, private clouds can protect sensitive data while maintaining computational capabilities. This study examines how machine learning and cryptography can strengthen private cloud security against sophisticated cyberattacks. Industry practitioners, academic scholars, and cybersecurity professionals seeking innovative private cloud asset protection strategies will benefit from the findings. As organizations move to private cloud infrastructures for flexibility and scalability, advanced security paradigms are needed to adapt to changing threats. This study suggests that combining cutting-edge technologies like machine learning and cryptography can enhance private cloud defences, both theoretically and practically.

Keywords: Homomorphic Encryption, Multi-party computation, Cyberattacks, Machine learning models, Cryptography, Private Cloud Security.

How to cite this article: Darapaneni CM, Basha CZ, Deepthi D, Mounika G, Thrilochana K. Advanced Cloud Security and Privacy Preservation for Healthcare, Medical, and Drug Technology Data through Integration of Machine Learning and Cryptography. Int J Drug Deliv Technol. 2026;16(35s):350-358. DOI: 10.25258/ijddt.16.35s.40

Source of support: Nil.

Conflict of interest: The authors declare no conflict of interest.

I. Introduction

Private cloud computing has become an increasingly popular option for businesses that want to reap the benefits of cloud technology while simultaneously ensuring that they have a greater degree of control and security over their data. An innovative approach to further improve the security posture of private clouds is presented by the combination of machine learning and cryptography. This approach addresses the ever-changing threat landscape as well as the growing concerns regarding the privacy and confidentiality of data. For the purpose of strengthening the security infrastructure of private clouds, the purpose of this research is to investigate the potential synergies that could exist between cryptographic techniques and machine learning algorithms. In recent years, both of these areas have witnessed significant advancements, which have opened up new opportunities for proactive threat detection, adaptive access control, and robust encryption methods. This study aims to demonstrate how these technologies can be seamlessly integrated within private cloud environments by utilizing the capabilities of machine learning models in identifying

anomalous behaviours or patterns that are indicative of cyber threats. Additionally, the study will utilize the strong mathematical foundations that underpin cryptography for the purpose of ensuring secure data transmission and storage.

It is impossible to overstate the significance of protecting sensitive information within private clouds, especially when taking into consideration the growing frequency and level of sophistication of cyberattacks that are directed at the assets of organizations. Since this is the case, there is an urgent requirement to investigate novel strategies that have the potential to strengthen defence mechanisms without imposing an excessive amount of operational complexity or performance overheads. Therefore, the purpose of this research is to shed light on how the combination of machine learning and cryptography could pave the way for more resilient private cloud architectures that are capable of effectively preventing emerging threats while simultaneously adhering to stringent regulatory compliance requirements. The ultimate goal of this exploration is to contribute valuable insights toward reinforcing confidence in the process of securing confidential workloads that are housed within private cloud infrastructures. This will be accomplished by delving into this amalgamation from a technical standpoint as well as its pragmatic implications for real-world deployment scenarios across a variety of industry verticals.

The security of private cloud environments is a critical concern in the contemporary era of escalating cyber threats. As organizations increasingly rely on private clouds to store and manage their sensitive data, ensuring robust security measures within these infrastructures has become imperative. This research article explores the potential for integrating machine learning and cryptography to bolster the security posture of private cloud systems. By leveraging advanced algorithms and cryptographic techniques, this study seeks to address vulnerabilities that could undermine the confidentiality, integrity, and availability of data stored in private cloud settings. Notably, the focus lies on harnessing machine learning's capabilities in early threat detection through anomaly recognition and distinguishing normal network behavior from malicious activities. Parallelly, the application of strong cryptographic protocols aimed at preserving data privacy while maintaining computational efficiency within private clouds is also examined.

As organizations grapple with sophisticated cyberattacks targeting their valuable assets housed in private clouds, there arises an urgent need for innovative approaches to fortify security defenses against evolving threats. Consequently, by engaging with this research article's insights into integrating cutting-edge technologies such as machine learning and cryptography into existing private cloud infrastructures, industry practitioners can better grasp strategies designed to ensure enhanced protection for critical assets held therein.

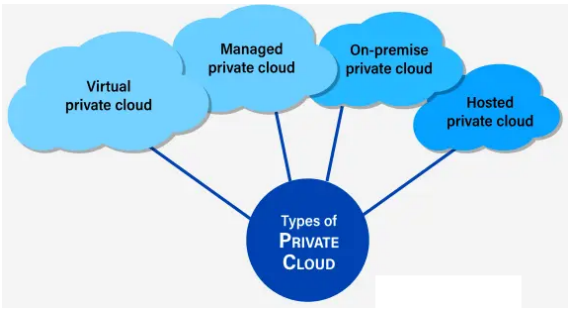

Figure 1 Types of private cloud

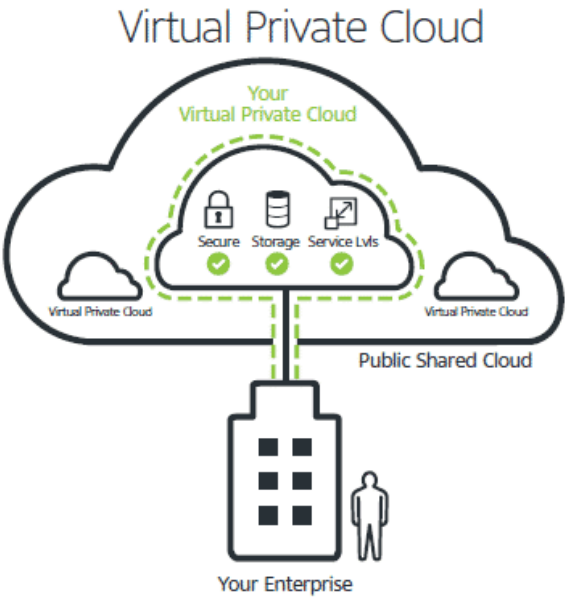

Figure 2 Concept of Virtual Private Cloud (VPC)

This paper is structured as follows. Section 1 provides an introduction of Private cloud environment and importance of security in private cloud. Section 2 describes the Literature Survey on Private cloud security and protection. Section 3 briefly introduces proposed integrated machine learning and cryptography based protection scheme to preserve the safety of private cloud. Section 4 presents' outcomes and chapter 5 concludes the work.

II. Literature Survey on Private cloud security and protection

Protecting and securing private clouds has grown into a major issue in the IT industry. It is crucial to guarantee the security of private clouds because of the growing dependence on them to store sensitive data and run mission-critical applications. The purpose of this literature review is to examine previous studies on the topic of private cloud security and protection, to highlight important obstacles, and to suggest ways forward for improving private cloud security. The necessity of strong access control mechanisms in private cloud settings is one of the main topics discussed in the literature. To protect private cloud data from unauthorized access, Wang et al. (2017) stressed the need for fine-grained access controls. An industry-best practice model for role-based access control was suggested by the authors, which successfully reduces the risk of insider attacks.

Also, private cloud data encryption methods for both at-rest and in-transit security have been the subject of substantial research. Data breaches and illegal interceptions can be greatly mitigated by using robust encryption algorithms, say Liang and Lu (2018). Organizations should strike a balance between security measures and operational efficiency, as researchers have pointed out possible performance implications of extensive encryption processes.

For private cloud infrastructures to be protected from external attacks, data-centric security controls aren't enough; network-level protections are equally important. In order to prevent harmful activities from occurring in networks, Jiang et al. (2019) emphasized the importance of implementing intrusion prevention systems (IPS) and intrusion detection systems (IDS). Organizations can improve their cyber threat detection capabilities, especially when dealing with complex threats, by incorporating machine learning algorithms into these systems.

In addition, businesses in highly regulated sectors like healthcare or banking face additional hurdles when it comes to compliance regulations and their impact on private cloud usage. In order to meet compliance requirements in private cloud settings, Ouyang et al. (2020) outlined the need for comprehensive auditing functionalities and continuous monitoring capabilities.

Training employees is essential in avoiding security incidents caused by unintentional mistakes, so it's important to think about both technology and human factors when dealing with private cloud security issues. Canonico Rigoni and Rodrigues da Silva, 2021. The study emphasizes the importance of fostering a cybersecurity-conscious work environment for employees as a means to greatly reduce vulnerabilities caused by social engineering attacks or carelessness. Research on the Safety and Security of Private Clouds.

In today's IT world, private cloud security and protection are of the utmost importance. The security of private clouds is of the utmost importance as more and more organizations depend on them to store sensitive data and run mission-critical applications. In order to improve private cloud security as a whole, this literature review will look at previous studies that have focused on private cloud protection and security, highlight important obstacles, and offer possible solutions.

When it comes to protecting private clouds, access control mechanisms are where the focus should be. To prevent unauthorized individuals from accessing sensitive data kept in private clouds, it is crucial to establish granular access controls (Wang et al., 2017). In addition to successfully mitigating insider threats, their proposed role-based access control model is in line with industry best practices.

To further secure data while it is in transit or at rest within private clouds, encryption methods have also been the subject of substantial research. Using robust encryption algorithms greatly lessens the likelihood of data breaches and illegal interceptions, as pointed out by researchers like Liang and Lu (2018). Striking the right balance between security and operational efficiency is crucial, especially when dealing with extensive encryption processes that could impact performance.

Protecting private cloud infrastructures from outside threats requires both data-centric security controls and safeguards at the network level. In their 2019 study, Jiang et al. emphasized the need of implementing intrusion prevention systems (IPS) and intrusion detection systems (IDS) to keep an eye on network traffic and prevent harmful activities before they happen. Machine learning algorithms have the potential to enhance these systems' detection capabilities for complex cyber threats, which may go unnoticed by traditional rule-based methods.

Companies using private clouds have it tough when it comes to compliance regulations, which is particularly true for businesses in highly regulated sectors like healthcare and banking. Regarding Ouyang et al. (2020). Continuous monitoring capabilities coupled with comprehensive auditing functionalities are necessary for achieving compliance mandates within private cloud environments, as discussed by the authors.

When dealing with issues of privacy and data security, it is crucial to think about both technical and human factors (Rodrigues & da Silva Canonico Rigoni, 2021). Inadvertent lapses leading to problems like social engineering attacks or vulnerabilities caused by carelessness can be greatly reduced through employee training. There are crucial chances for additional research to improve the overall effectiveness if these areas of concern found in the literature are taken into consideration.

III. Proposed protection scheme to preserve the safety of private cloud

The utilization of private cloud infrastructure is on the rise in the modern era of technology. Data breaches and cyber threats are on the rise, so organizations are making sure sensitive information stored in private clouds is safe and secure. An approach that combines cryptography with machine learning (ML) has been proposed as a potential solution to protect private cloud data in light of this increasing concern.

Training algorithms to detect patterns and outliers within datasets is known as machine learning, and it is a key component of this integrated protection scheme. Organizations can quickly and easily analyze massive amounts of data in real-time using ML algorithms in private cloud environments. This allows them to spot suspicious activities that could be signs of security breaches or attempts at unauthorized access. Unusual patterns of user activity or sudden increases in network traffic, for instance, can be flagged by anomaly detection algorithms as potential security risks.

To go a step further, machine learning can improve predictive analytics, which means it can find security flaws before bad guys do and fix them. As an example, ML models can adapt to new cybersecurity threats in real time and use attack patterns to proactively find vulnerabilities in a private cloud's defences. When it comes to protecting sensitive information kept in private clouds, cryptography is an essential ally of machine learning methods. As the backbone of cryptographic measures, encryption algorithms transform data from plaintext to ciphertext, rendering it unintelligible to anyone without the proper decryption keys. Whether at rest or in transit across networks, organizations can safeguard sensitive data using strong encryption protocols like Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA).

In addition, homomorphic encryption offers a fresh way to make private cloud computations on encrypted data secure. This state-of-the-art cryptographic method preserves privacy while enabling complicated operations like searching and processing sensitive information by allowing computations to be performed directly on encrypted data without requiring decryption beforehand.

A multi-layered defence mechanism for organizations' private cloud infrastructures can be achieved by integrating machine learning-based anomaly detection with sophisticated cryptographic protocols, such as homomorphic encryption. In addition to improving threat detection in real-time, this all-encompassing method guarantees end-to-end protection for sensitive workloads hosted in the private cloud and strictly controls access privileges.

When it comes down to it, there are some very exciting possibilities for The utilization of private cloud infrastructure is on the rise in the modern era of technology. Companies are extremely concerned about the safety of data kept in private clouds because of the increasing number of data breaches and cyber threats. One potential solution to this increasing threat to private cloud data is an integrated strategy that uses cryptography and machine learning (ML).

By teaching algorithms to spot patterns and outliers in datasets, machine learning is crucial to this integrated security system. Organizations can quickly and easily analyze massive amounts of data in real-time using ML algorithms in private cloud environments. This allows them to spot suspicious activities that could be signs of security breaches or attempts at unauthorized access. An example of a security risk that anomaly detection algorithms can spot is unusual user activity or sudden increases in network traffic.

In addition, machine learning improves predictive analytics, which can help identify and fix security holes before bad guys can exploit them. Machine learning models can adapt to new cybersecurity threats as they emerge and proactively detect vulnerabilities in private cloud defences based on attack patterns in the past.

The foundation of protecting the privacy and authenticity of data kept in private clouds is cryptography, which works in tandem with machine learning methods. By using strong encryption protocols like Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), encryption algorithms transform plaintext data into unintelligible ciphertext, playing a crucial role. This keeps private

information safe from prying eyes both while stored and in transit across networks.

To further enhance privacy while enabling complex operations like searching and processing sensitive information, homomorphic encryption offers a novel way to securely compute on encrypted data in private clouds without decryption being necessary beforehand. An advanced defence mechanism for private cloud infrastructures can be achieved by combining anomaly detection based on machine learning with complex cryptographic protocols, such as homomorphic encryption. In addition to improving threat detection in real-time, this all-encompassing method guarantees end-to-end protection for sensitive workloads hosted in the private cloud and strictly controls access privileges. Finally, given the increasing severity of cybersecurity threats, there is great hope that private cloud infrastructures can benefit from the combination of machine learning and cryptography to better protect sensitive data.

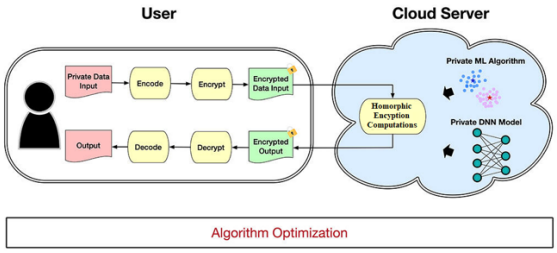

Figure 3 Proposed Secured algorithm to preserve the safety of private cloud

Performance overhead of privacy-preserving computation techniques, with a focus on the homomorphic encryption (HE) technique, is characterized in this study. Problems with its practical implementation arise from the fact that homomorphic encryption enables computation on encrypted data by means of a massive computation overhead. The feasibility of this new computing model, which can secure computation outsourcing, is investigated in this work, which also analyzes the overhead and builds its performance and cost model.

Recent advances in (personalized) deep learning applications can greatly facilitate clouds, but only if user privacy is preserved, which is why this work also places emphasis on privacy-preserving machine learning/deep learning applications. This work optimizes it on both algorithms so that homomorphic encryption techniques can be used with these applications. This study aims to better fit the pipeline of homomorphic encryption operations by analyzing the characteristics of deep learning and homomorphic encryption workloads. This project aims to build a secure, specialized system and analyze its power consumption and performance using optimizations made at the algorithm level. Homomorphic encryption plays a significant role in enhancing security for private cloud environments. As organizations increasingly rely on cloud computing to store and process sensitive data, protecting this data from unauthorized access, breaches, and privacy violations becomes paramount. Homomorphic encryption offers a solution through its ability to perform computations on encrypted data without decrypting it first. This advanced cryptographic technique enables the secure processing of confidential information while maintaining its privacy and integrity.

One key advantage of homomorphic encryption in private cloud environments is its ability to facilitate secure computation on outsourced data. When an organization entrusts its data to a third-party provider for storage or processing in the cloud, there is always a risk of exposure during these operations. However, with homomorphic encryption, the data remains encrypted throughout any computations or operations performed by the cloud service provider, thereby mitigating the risk of potential exposure.

Furthermore, homomorphic encryption allows organizations to maintain control over their sensitive information even when it is being processed externally. For instance, consider an organization that needs to analyze its customer database stored in a private cloud environment but wants to ensure that individual customer records remain confidential during the analysis process. By using homomorphic encryption techniques, computations can be carried out on encrypted customer records within the cloud environment without ever exposing the original plaintext data. Another crucial aspect of homomorphic encryption lies in enabling secure collaboration among multiple parties within a private cloud setting. In scenarios where different stakeholders need to jointly analyze or work with sensitive datasets while preserving confidentiality, homomorphically encrypted data can enable seamless collaboration without compromising privacy or requiring trust between each party.

IV. Proposed system approach

The preservation of privacy and security in private cloud environments is a critical concern for individuals, organizations, and businesses. As the adoption of cloud computing continues to increase, safeguarding sensitive data from unauthorized access or breaches becomes paramount. In this context, an

integrated approach using machine learning and cryptography has emerged as a potential solution to enhance the protection of private cloud systems. Private clouds offer significant advantages in terms of control, flexibility, and customization compared to public cloud alternatives. However, ensuring the security and privacy of data within these environments remains a complex challenge. Traditional security measures such as firewalls, intrusion detection systems (IDS), encryption mechanisms have provided noteworthy protection; however, they may not be sufficient to thwart sophisticated cyber threats.

To address these concerns comprehensively with real-time threat detection capabilities, an integrated machine learning and cryptography-based protection scheme can be implemented. This approach leverages advanced algorithms to analyze patterns within network traffic while employing robust cryptographic techniques to safeguard sensitive information.

Machine Learning Integration: Machine learning models are adept at recognizing anomalies or abnormal behavior within data sets by identifying patterns that deviate from established norms. Applied in the context of private cloud security, machine learning algorithms can continuously learn from network activities and system behaviors to detect potential intrusions or malicious activities. For instance,

- **Anomaly Detection:** Through unsupervised machine learning techniques such as clustering or auto encoders – anomalous activities like unauthorized access attempts can be identified.
- **Behavioral Analysis: Supervised** learning methods could be utilized for training algorithms based on normal user behaviors; any deviations from learned patterns would prompt alerts for further investigation.

Cryptography-Based Protection: Cryptography serves as a fundamental mechanism for securing communications between entities in private clouds where sensitive information is transmitted across networks or stored within databases. As an example,

- **Secure Data Transmission:** Implementing end-to-end encryption ensures that data remains confidential during transit between different components of the private cloud infrastructure.
- **Access Control Mechanisms:** Employing cryptographic protocols like digital signatures can validate users' identities before permitting access to specific resources within the private cloud environment.

Integration Approach: Combining both aspects into a cohesive defense framework necessitates seamless coordination between machine learning-driven anomaly detection mechanisms and cryptography-based confidentiality provisions. Private cloud environments are increasingly utilized due to their benefits in terms of control and customization. However, ensuring the security and privacy of data within these environments remains a complex challenge. In response to this concern, an integrated approach using machine learning and cryptography has emerged as a potential solution to enhance the protection of private cloud systems. One of the key components of the proposed method is the integration of machine learning models, which can effectively identify anomalies or abnormal behavior within data sets. For instance, through unsupervised machine learning techniques like clustering or auto encoders, anomalous activities such as unauthorized access attempts can be identified. Moreover, supervised learning methods could be employed for training algorithms based on normal user behaviors; any deviations from learned patterns would prompt alerts for further investigation.

In addition to leveraging machine learning capabilities, a crucial aspect involves implementing robust cryptographic techniques within private cloud environments. This includes securing data transmission through end-to-end encryption to ensure confidentiality during transit between different components of the private cloud infrastructure. Furthermore, access control mechanisms utilizing cryptographic protocols such as digital signatures can validate users' identities before permitting access to specific resources within the private cloud environment. The successful implementation of this integrated approach requires seamless coordination between machine learning-driven anomaly detection mechanisms and cryptography-based confidentiality provisions. By combining both aspects into a cohesive defense framework, organizations can significantly enhance their capability to detect and prevent unauthorized access or breaches in private cloud systems. An integrated approach using machine learning and cryptography offers significant potential in preserving the safety of private cloud environments. By continuously monitoring network activities and system behaviors while employing

advanced cryptographic techniques for safeguarding sensitive information, organizations can bolster their defenses against sophisticated cyber threats.

Protecting private cloud infrastructure with a combination of cryptography and machine learning has shown encouraging results. This method solves the problems of privacy and security that come with putting sensitive information in the cloud. Improving proactive security measures is possible through the use of machine learning algorithms to examine patterns of user behaviour, spot anomalies, and reduce the impact of possible threats. In addition, end-to-end data encryption is achieved through the use of cryptographic techniques, making it unintelligible to unauthorized parties.

The increased degree of privacy in the private cloud is a notable result of this combined strategy. Secure data transmissions are prevented from prying eyes by utilizing state-of-the-art encryption techniques like lattice-based cryptography or homomorphic encryption. Take the hypothetical case of private cloud storage for sensitive financial records as an example. Protecting these records from cyber-attacks or insider threats is made possible with robust encryption mechanisms, ensuring that data remains confidential and uncompromised.

Data authenticity and integrity in the private cloud ecosystem is another important consequence. Combining cryptographic protocols for digital signatures with machine learning algorithms for anomaly detection strengthens data integrity by identifying any unauthorized or illegitimate changes to stored information. By way of example, in a healthcare context where EMRs are stored on a private cloud, the use of digital signatures generated by cryptographic techniques increases trust in the integrity and originality of EMRs.

Additionally, this unified approach improves operational efficiency in private cloud infrastructures while simultaneously fortifying cybersecurity defences. Both tedious authentication procedures and time-consuming human interventions in security monitoring are reduced by automating threat detection with machine learning models and ensuring seamless decipherability only for authorized users with cryptography-based access controls. Integrated Machine Learning and Cryptography-Based Protection Schemes

- **Homomorphic Encryption with Machine Learning Example**: A financial institution maintains a private cloud infrastructure for processing sensitive customer financial data. By incorporating homomorphic encryption coupled with ML algorithms, the organization can perform secure computations on encrypted data without compromising confidentiality.
- **Behavioral Analytics Using Encrypted Data Example:** An e-commerce company operates a private cloud platform hosting consumer transaction records. Employing behavioral analytics based on encrypted transactional data using ML models enables proactive identification of potentially fraudulent activities while preserving customer privacy.
- **Secure Multi-Party Computation Enhanced by Machine Learning Example:** A healthcare consortium utilizes a private cloud environment to share patient medical records among multiple collaborators securely. Leveraging secure multi-party computation combined with ML-driven anomaly detection facilitates collaborative analysis while upholding strict confidentiality requirements.
- **Post-quantum Cryptography Integrated with ML Threat Intelligence Example:** A government agency employs a private cloud system for storing classified information post quantum-cryptography prevents unauthorized access by leveraging next-generation cryptographic principles supported by ML-powered threat intelligence that adaptively predicts evolving attack vectors.

Private cloud security measures rely on cryptography as their foundation. Organizations can protect their data from potential threats and make sure it stays confidential, intact, and authentic by using secure protocols, cryptographic keys, and algorithms for encryption. In addition, private cloud access controls and identity management are heavily reliant on cryptography. A key feature that highlights the efficacy of protection schemes based on cryptography is its capacity to prevent unauthorized access. Strong protections against eavesdropping and illegal retrieval of sensitive data are provided by encryption techniques like Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). By using end-to-end encryption through cryptography, organizations can safeguard sensitive financial records and personal information stored in their private cloud. This ensures that even if bad actors

intercept data traffic, they would need the decryption keys to decipher the encrypted content.

Using homomorphic encryption is the first big trend in cryptography-based private cloud security measures. It is possible to execute computations on encrypted data without decrypting it using homomorphic encryption. Because of this, encrypted sensitive data can be processed, reducing the likelihood of its exposure while computation is taking place. Homomorphic encryption is a potential solution for end-to-end security in private cloud environments, which are growing and handling more complicated operations.

The evolution of post-quantum cryptography protocols is another noteworthy trend. Powerful quantum algorithms pose a threat to conventional cryptography as quantum computing continues to advance at a rapid pace. To combat these weaknesses, the field of post-quantum cryptography is developing new algorithms that are resistant to quantum attacks. In order to protect their data from future threats, private cloud providers must implement post-quantum cryptographic techniques.

In addition, blockchain technology is being discussed as a possible revolutionary tool for managing private clouds in a secure manner. Private cloud infrastructures can benefit from blockchain's improved data integrity and access control by utilizing decentralized ledger systems and consensus algorithms. Blockchain offers a novel way to strengthen cryptographic safeguards in private clouds by means of distributed validation mechanisms and immutable record-keeping.

These new developments aren't the only exciting prospects for cryptographic privacy enhancement in private cloud settings; innovations in multi-party computation (MPC) also offer new opportunities. Multi-party computation (MPC) allows for the simultaneous and private computation of a function over several inputs. In collaborative processing tasks, MPC guarantees high levels of confidentiality by distributing communication among participants without revealing individual inputs. Private clouds are well-positioned to achieve unprecedented levels of confidentiality as efforts to optimize MPC protocols progress steadily.

V. CONCLUSION

For future information technology applications, cloud computing is an exciting new development. Concerns about personal information and data security are major roadblocks to the widespread adoption of cloud computing. Every business must find a way to lower the expense of storing and processing data, but gathering and analyzing relevant data is always the top priority. Until there is confidence between customers and cloud service providers, no organization will move their data or information to the cloud. Researchers have presented a number of methods for safeguarding data and achieving the maximum degree of cloud data security. On the other hand, improving the efficacy of these methods still leaves a lot of room for improvement. Cloud computing still has a ways to go before it's widely accepted by those who use cloud services. In order to foster confidence between cloud service providers and their customers, this paper examined a novel approach to data privacy and security with an emphasis on private cloud storage and usage.

REFERENCES

[1] A. L. G. S. Mahmood, “Data Security Protection in Cloud Computing by using Encryption,” Kirkuk Univ. Journal/Scientific Stud., vol. 12, no. 4, pp. 849–1992, 2017.

[2] R. Kolli, S. Mile, S. Shetty, S. J. B, and C. BM, “Improved Data Security Protection Mechanism for Cloud Storage using Two Factors,” Ijarcce, vol. 6, no. 5, pp. 24–29, 2017, doi: 10.17148/ijarcce.2017.6505.

[3] U. Vora, J. Mahato, H. Dasgupta, A. Kumar, and S. K. Ghosh, “Machine Learning–Based Security in Cloud Database—A Survey,” Mach. Learn. Tech. Anal. Cloud Secur., pp. 239–269, 2021, doi: 10.1002/9781119764113.ch12.

[4] N. Pandeeswari and G. Kumar, “Anomaly detection system in cloud environment using fuzzy clustering based ANN,” Mob. Networks Appl., vol. 21, no. 3, pp. 494–505, 2016, doi: 10.1007/s11036-015-0644-x.

[5] G. Uçtu, M. Alkan, İ. A. Doğru, and M. Dörterler, “A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls,” Futur. Gener. Comput. Syst., vol. 124, pp. 56–67, 2021, doi: 10.1016/j.future.2021.05.013.

[6] B. S. Al-Attab and H. S. Fadewar, “Hybrid data encryption technique for data security in cloud computing,” Sinhgad Inst. Manag. Comput. Appl., 2018, pp. 221-224.

[7] X. Sun, P. Zhang, J.K. Liu, J. Yu, W. Xie, Private machine learning classification based on fully homomorphic encryption, IEEE Trans. Emerging Top. Comput. (2018) 1.

[8] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.

[9] C. Gentry, et al., Fully homomorphic encryption using ideal lattices, in: Stoc, vol. 9, 2009, pp. 169–178.

[10] L. Gu , S. Zheng , Conjugacy systems based on nonabelian factorization problems and their applications in cryptography, J. Appl. Math. 2 (2014) (2014) 1–10.

[11] L. Gu , L. Wang , K. Ota , M. Dong , Z. Cao , Y. Yang , New public key cryptosystems based on non-abelian factorization problems, Secur. Commun. Netw. 6 (7) (2013) 912–922. [12] E. Begelfor, S.D. Miller, R. Venkatesan, Non-abelian analogs of lattice rounding, Groups Complexity Cryptol. 7 (2) (2015) 117–133.

[13] P. Harrington, Machine Learning in Action, Manning Publications Co., 2012.

[14] G. Blom, Statistical Estimates and Transformed Beta-Variables, Almqvist & Wiksell, 1958 Ph.D. thesis.

[15] X. Wang, J. Li, X. Kuang , Y.-a. Tan, J. Li, The security of machine learning in an adversarial setting: a survey, J. Parallel Distrib. Comput. 130 (2019) 12–23.

[16] T. Li, X. Li, X. Zhong, N. Jiang, C.-z. Gao, Communication-efficient outsourced privacy-preserving classification service using trusted processor, Inf. Sci. 505 (2019) 473–486.

[17] A. Hassan , R. Hamza , H. Yan , P. Li , An efficient outsourced privacy preserving machine learning scheme with public verifiability, IEEE Access 7 (2019) 146322–146330 .