A Comprehensive Analysis of Cloud Data Storage and Security: A Narrative Review

Ravanan Sundari Kanakasabapathi and John Edwin Judith

ABSTRACT

Microsoft, Amazon, and Google, among others, are leading the way in creating and offering advanced cloud computing systems at a low cost. Cloud computing's largest security issue prevents people from embracing it. Cloud computing infrastructure security is crucial. Cloud infrastructure security research has addressed certain holes, but new issues keep arising. This systematic literature review (SLR) examines research on security, availability, integrity, confidentiality, network security, and cloud security concerns. This SLR assessed prominent digital libraries' 2017–2022 research studies. After careful screening, we chose 115 publications to address the study questions. Secure communication may be achieved by encrypting cloud data. This research also examined some key issues that make cloud security engineering difficult.

Keywords: Attribute-based encryption, Homomorphic encryption, Identity-based encryption, Nature-inspired cryptographic optimization, Cloud storage security challenges

Computer Applications, Nooral Islam centre for Higher Education, Kumarakoil, Nagercoil, Tamil Nadu, India

Correspondence to: Ravanan Sundari Kanakasabapathi, sabapathiravanan93@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Kanakasabapathi RS and Judith JE. A Comprehensive Analysis Of Cloud data storage and security: A Narrative Review. Premier Journal of Science 2025;15:100206

DOI: https://doi.org/10.70389/PJS.100206

Peer Review

Received: 14 August 2025

Last revised: 26 September 2025

Accepted: 17 December 2025

Version accepted: 2

Published: 9 January 2026

Ethical approval: N/a

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution: Ravanan Sundari Kanakasabapathi and John Edwin Judith – Conceptualization, Writing – original draft, review and editing

Guarantor: Ravanan Sundari Kanakasabapathi

Introduction

Cloud computing (CC) uses Internet networks to access computational resources. Cloud computing offers cheap, on- demand services. Cloud computing changed IT because of its resource sharing, multi-tenancy, and distant data sharing.[1–3] Cloud computing provides rapid, simple processing and data storage. Cloud computing uses IAAS, PAAS, and SAAS service paradigms (SAAS). IAAS gives consumers compute and storage to boost their companies. PAAS providers give consumers software tools to do their jobs. A cloud service provider deploys SAAS software and data, which customers access online.[4,5] Cloud computing technology stores text, music, video, and images. Cloud computing expands IT capabilities without additional infrastructure, software licencing, or staff training.[6,7]

WhatsApp, Microsoft Office 365, Google Docs, and Skype, as well as CRM and ERP software, allow us to access our data from anywhere.[8,9] Cloud computing has ubiquitous network connectivity, quick resource flexibility, self-service, risk transfer, location-independent resource pooling, and usage-based pricing. Cloud computing's benefits have attracted academic research and industry.[10,11] CC offers exciting IT applications, but various difficulties must be solved to install and store data in a CC environment. Data security and privacy threaten CC services. Encryption is used to secure cloud data.[12,13] Data security has always plagued IT. Security hinders cloud computing adoption. Trust, Compliance, Privacy, Integrity, and legal challenges comprise security.[14,15] Institutions and cloud computing evolve with integrity and privacy. Because data is disseminated among servers, PCs, and mobile devices such as smart phones and WSNs, cloud computing raises data integrity and privacy concerns.[16,17] Security ensures cloud data dependability and network transfer. Figure 1 shows the review protocol of databases, search strings, selection flow, quality assessment etc.

Cryptography protects sensitive data against unwanted access.[18] Symmetric-key cryptography, where the transmitter and receiver share the same encryption and decryption key, is one of two basic encryption methods (the other is private key encryption). AES, Blowfish, DES, IDEA, etc. (b) public-key cryptography, which uses distinct keys for encryption and decryption. Asymmetric key cryptography is RSA. Figure 2 depicts cloud computing.

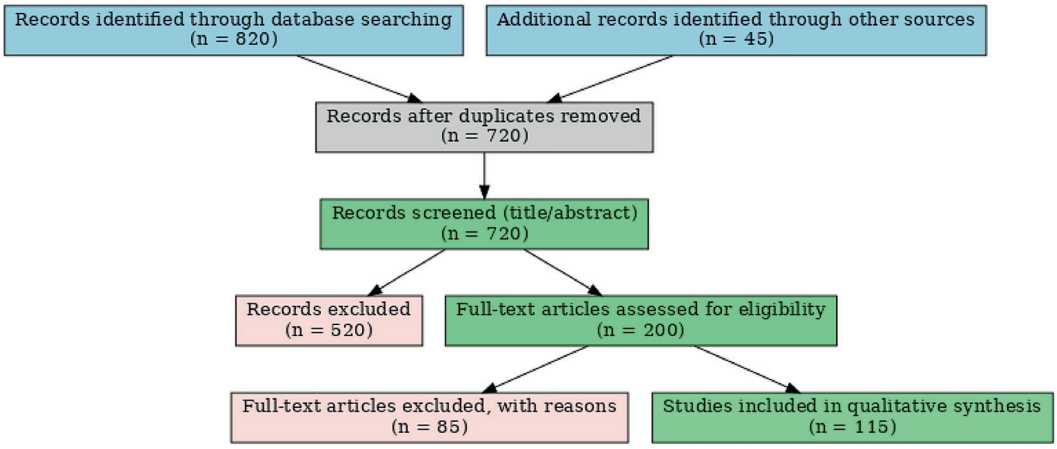

Fig 1 | PRISMA flow diagram

Provenance and peer-review: Unsolicited and externally peer-reviewed
Data availability statement: N/a

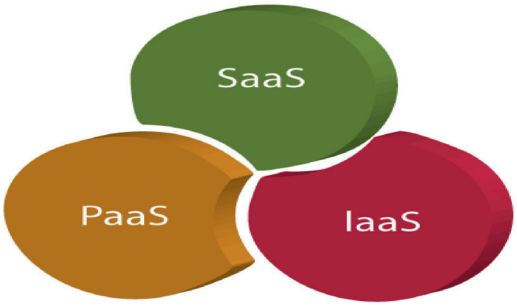

Fig 2 | Model of cloud computing

Encryption of Cloud Data via Post-Quantum

The rapid pace of quantum computing research is a real threat to the already established public-key cryptosystems such as the RSA and elliptic curve cryptography that are the foundation of the security of the current cloud stores. To ensure safety of sensitive information and its integrity in the coming few decades, cloud service providers must go to post-quantum cryptography (PQC). This section contains the critical review of three major approaches such as lattice-based attribute based encryption, hybrid post-quantum key encapsulation mechanism (KEMs) with symmetric encryption, and post-quantum homomorphic encryption, with respect to its use in cloud storage systems.

PQ-ABE Lattice-Based Attribute-Based Encryption

Lattice-based cryptography, rooted in the Learning With Errors (LWE) problem, forms one of the most promising families of quantum-resistant schemes.[19,20] To provide fine-grained access control, allowing user attribute or user-role based encryption policies have lattice constructions been added to attribute-based encryption (ABE). This provides a single ciphertext in cloud storage with the capability of being safely shared among the many authorized users without encryption repetition. The new lattice-based ciphertext-policy ABE constructions have increased quantum attack resistance, without reducing expression policy enforcement. The cost is however rewarded: ciphertexts and secret keys are significantly larger, and the requirements are greater than classical ABE.[21,22] Two of the issues that have not been addressed effectively are key management and revocation processes that can be scaled to deploy lattice-based ABE in large-scale applications in the cloud environment.

Symmetrically Encrypted Hybrid PQ KEMs

Employing hybrid designs of post-quantum KEMs with already verified symmetric algorithms such as AES is a short-term pragmatic strategy of cloud providers. In this case, the implementation of key exchange is realized by a quantum-safe KEM (e.g. CRYSTALS-Kyber, which is standardized in 2022 by NIST), and bulk data encryption with efficient symmetric ciphers. This approach gives it a reasonably smooth Migration path because it integrates into the existing TLS protocols, key management providers and storage architectures.[23,24] The benefits lie in its simplicity in terms of installing and deploying, low performance and high adherence to international standards. This is limited by the fact that it is not accompanied with access policy enforcement, the policy management still has to be founded on traditional authentication and authorization schemes.[25,26]

Post-Quantum Homomorphic Encryption (PQ-HE)

Homomorphic encryption enables the computation of encrypted data, which is a precious characteristic of data privacy-protective analytics in multi-tenant clouds. The lattice-based fully homomorphic encryption (FHE) is quantum-resistant and it can also process ciphertexts.[27–29] In the case of cloud storage, this would enable the organizations to not only outsource data storage, but also processing without the exposure of plaintext. However, PQ-HE remains computationally infeasible: the ciphertext size is hundreds of times larger than the plaintext size, and real-time throughput has not yet been realized by large-scale applications. PQ-HE research prototypes are real and efficient, but require significant efficiency enhancements before becoming useful in non-niche applications.

Comparative Assessment

- ABE lattice-based is solid in policy enforcement but suffers scalability and efficiency issues.
- Hybrid PQ KEMs provide a short period, deployable solution to protect data in transit and key management with negligible disruption.
- PQ-HE provides the most powerful but it does not apply to general cloud storage.

Informational Background on the use of Cloud Computing

Could computing provides on-demand access to end users' resources, including data storage and computing power, without a client- specific relationship. The word refers to Internet-accessible server farms. Today's massive clouds have restrictions that central servers disregard. Edge servers may be deployed for customers with good relationships. We summaries relevant research.

Cloud-Service Models

Observing company performance is crucial as cloud infrastructures are increasingly used to provide IT services. Cloud providers may disclose subjective system execution data, limiting productive cloud selection,

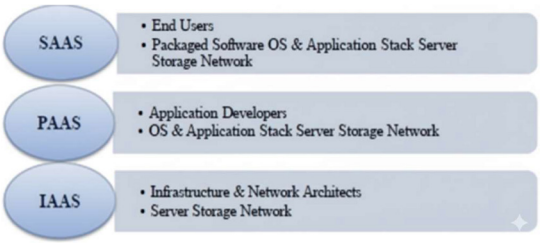

Fig 3 | Level of cloud service

DOI: https://doi.org/10.70389/PJS.100206 | Premier Journal of Science 2025;15:100206

raising performance concerns, creating vulnerabilities in assisted administrations, and leading to poor deployment decisions. IAAS, SAAS, and PAAS are CC service models. Cloud models help different enterprises (Figure 3).

Software As A Service (SAAS)

The typical software distribution model involves a third- party host that provides online accessibility to a program. Billing and invoicing, CRM, and support desk SAAS apps arepopular. SAAS eliminates the need for installation, setup, administration, and hardware maintenance, among other benefits. Most of these services are utility- or subscription- based and easily accessible. Thus, it is cheaper than licenced apps. Service providers handle software and hardware upgrades, decreasing end-user strain. Control, security, network dependencies, switching, and multitenancy are the primary problems.

Platform as a Service (PAAS)

PAAS offers runtime environments, programming, and application development. It delivers an operating system, middleware, servers, software frameworks, database, and computing environments for specific purposes as a service. Developers no longer have to painstakingly buy the primary gear and deal with administration, configuration, and infrastructure setup. PAAS supports instrumentation, application versioning, state management, scalability, storage, persistence, security, database integration, web services, deployment, testing, design, and application development. Windows Azure, Google App Engine, Heroku, and Force.com are popular PAAS providers. They support several programming languages for user convenience. Google App Engine lets developers choose between Java and Python. Azure supports Java, Ruby, and. NET. Heroku runs Ruby on Rails web apps. Force.com features two languages: Apex, a Java-like language, and Visual Force, an Excel-like query language.

- This service has risks too. SAAS' biggest challenges:
- Security, Data Lock-in, Resource Efficiency

Infrastructure as a Service (IAAS)

This technique displays the hardware needed for computing as a service. Web-based VMs, routers, servers, and storage are the most frequent facilities used. Unlike conventional hosting services, IAAS providers rent virtual machines on a utility model. This versatile, economical method scales. The user may administer the VM, controlling when it runs, installing programmes and software, and managing a custom OS. Amazon Web Services' Elastic Compute Cloud (EC2) is the most popular IAAS (AWS). Microsoft Azure, GCE, Net Magic Solutions, and Rack Space are some examples. Despite its benefits, this has drawbacks. network dependencies, prompt VM updates, and legacy security vulnerabilities. Table 1 shows the cloud computing services delivery models responsibilities.

Table 1 | Cloud computing services delivery models responsibilities

SAAS	Application	Data	Runtime	Middleware	Operating System	Virtualization	Hardware
PAAS	Application	Data	Runtime	Middleware	Operating System	Virtualization	Hardware
IAAS	Application	Data	Runtime	Middleware	Operating System	Virtualization	Hardware

Cloud Deployment Models

Private, public, hybrid, community, and multi-clouds make up the deployment model, regardless of service type. Figure 4 shows the cloud computing deployment model.

Private Cloud

Typically, this type of cloud is owned by a single organization and customized to meet its specific requirements. Organizations can achieve greater control over their data and potentially meet regulatory compliance requirements by utilizing private cloud storage. The data could consist of various types of sensitive information, such as medical records, trade secrets, or classified data. The same organization controls and operates the infrastructure. The private cloud requires a high level of security compared to other cloud environments. Identifying and managing user and vendor information, as well as addressing security risks, is simpler in a private cloud compared to a public cloud.

Public Cloud

Various organizations are responsible for managing and maintaining a public cloud in this particular kind of cloud. Numerous organizations and individuals utilize these networks, infrastructures, and resources simultaneously. Renowned public cloud providers include Microsoft, Amazon, and Google. Key concerns in this cloud type include data security, shared access management, ownership detection, and resource allocation against attacks.

Hybrid Cloud

Hybrid clouds combine private and public clouds to enable seamless transfer of services and applications between them. Hybrid cloud customers usually keep important apps on their own servers for more control

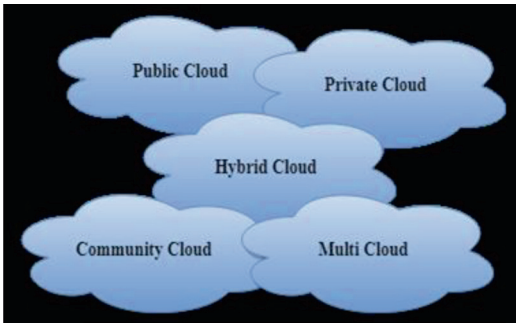

Fig 4 | Cloud computing deployment model

and security, while storing less critical apps at the cloud provider's location. Hybrid clouds allow business owners to easily expand their network infrastructure using the public cloud while maintaining access control, security, and data privacy in the private cloud. Hybrid cloud models are also superior for workloads that need to adhere to data security or compliance regulations.

Community Cloud

A community cloud enables multiple organizations to share systems and services for exchanging information within a specific community. The aim of this idea is to facilitate collaboration among various clients for community-owned projects and applications that require a centralized cloud platform. Community Cloud is a distributed infrastructure that combines various cloud services to address specific business sector needs. Hybrid clouds allow business owners to easily expand their network infrastructure using the public cloud while maintaining access control, security, and data privacy in the private cloud. The hybrid cloud model is a preferred choice for hosting workloads that need to comply with data security and compliance standards. Organizations can avoid security concerns associated with the public cloud by utilizing an exclusive user group. The community cloud is known for its scalability and versatility as it can be easily adapted to meet the requirements of various users. It offers compatibility with a wide range of users and can be customized accordingly.

Multi-Cloud

The term "multi-cloud" is used to describe the utilization of multiple public clouds. Utilizing multiple public clouds provided by various cloud providers within a company's infrastructure is known as a multi-cloud deployment. Instead of being dependent on a single vendor, a company in a multi- cloud configuration utilizes multiple vendors for cloud hosting, storage, and the complete application stack.

Characteristics of Cloud Computing

The technology of CC holds great promise for organizations as it enables them to securely transfer and expand their data from physical locations to a server in the cloud. This cloud server can be accessed from any location and at any time. CC offers various services to users regardless of their type, with the specific services provided being dependent on their specific needs and requirements.

Cloud Database

A database organises data. Multi-component cloud databases interact. It has a front and a rear end. The user's computer's application and networking system access the cloud on the front end. The back end includes cloud servers and data storage infrastructure. Cloud databases provide economics, performance, efficiency, software upgrades, document compatibility, group collaboration, and high storage. Figure 5 shows the big data enabled cloud environment.

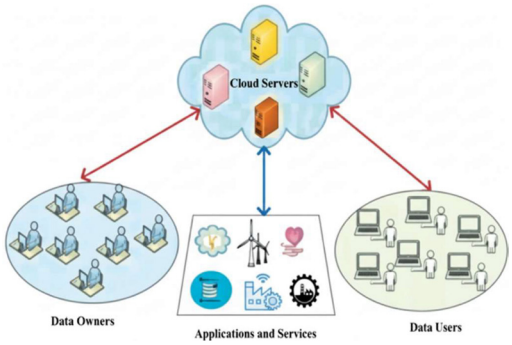

Fig 5 | Big data enabled cloud environment

Data Encryption Technology

Cloud data is insecure. Encryption secures data. Data encryption uses techniques to convert plaintext files or data into unreadable cypher text. The distorted code, even if accessed, ensures that the actual information remains inaccessible, thereby safeguarding its secrecy and preventing any unauthorized tampering. Users possessing the private key may decrypt the file and update the encrypted text. Asymmetric and symmetric encryption exist. Symmetric encryption employs a secret key. Symmetric encryption requires a consensus key, which makes file sharing difficult. Asymmetric encryption, specifically public-key encryption, provides more flexibility. Two keys are used in public-key encryption. Data can be encrypted using the public key, and the corresponding private key is used to decrypt the cipher text. We cover various popular cloud storage encryption methods in this section. Figure 6 demonstrates the taxonomy of the many encryption algorithms used for the security of cloud data.

Identity–Based Encryption

Data owners may safely outsource to an untrusted cloud server. Only authorised users have access to the IBE-cypher text-encrypted data on the server. By avoiding public-key certificates, all users, including consumers and data owners are identified by their unique identities. Figure 7 demonstrate the identity-based encryption for storage of data in the cloud.

The author introduced an upgraded identity-based encryption solution in that generates a safe key using part of an identity bit string to prevent identity leaks even if an opponent or attacker decodes the key or encrypted material. In, the author proposed a secure, lightweight cloud-based E- healthcare access method. To protect e-healthcare, provide stakeholders with a secure interface and prevent unauthorised individuals from accessing cloud data demonstrated an effective identity-based distributed decryption technique. Sharing data with many people without having to reconstruct the decryption private key is convenient proposes CP-IBE for cloud data. CP-IBE is identity-based data encryption. CP- IBE-ECC is a new public-key cryptography system that integrates the CP-IBE algorithm with ECC (CP-IBE-ECC). A brief overview of lattice-based post-quantum PO-IBEKS for cloud

DOI: https://doi.org/10.70389/PJS.100206 | Premier Journal of Science 2025;15:100206

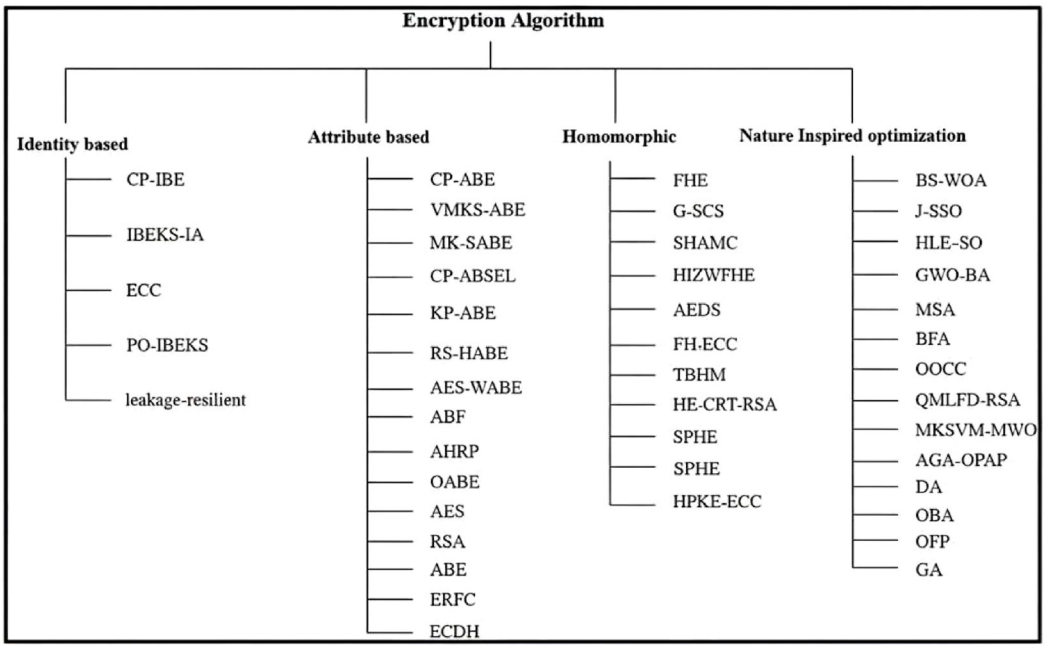

Fig 6 | A taxonomy of the many encryption algorithms used for the security of cloud data

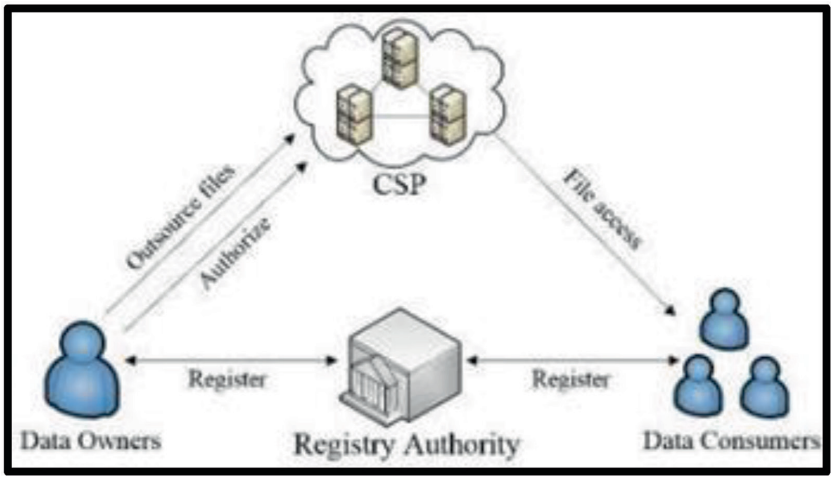

Fig 7 | Identity-based encryption for storage of data in the cloud

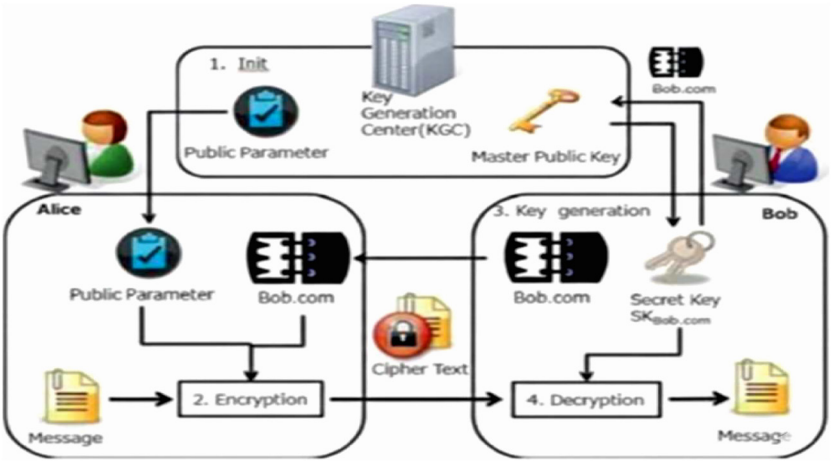

Fig 8 | Encryption based on attributes for use with cloud data storage

storage was provided. We conducted an investigation on IBEKS-IA, which is the first efficient identity-based broadcast encryption with keyword search, specifically aimed at preventing insider attacks in cloud database systems. IBEKS- IA retrieves data for numerous receivers and resists insider assaults. In, the authors created a leakage-resilient encryption scheme-based cloud computing and large data storage system. Our formal security proofs investigation shows that the suggested approach can protect customers' data even if cloud computing leaks the partial key.

Attribute–Based Encryption

Attribute-based encryption uses user characteristics as public keys.[33] Attribute-based encryption inherently includes identity-based encryption since user identification is an attribute. KP-ABE and CPABE are attribute-based encryptions. Figure 8 shows the encryption based on attributes for use with cloud data storage.

The authors introduced CP-ABSEL in cloud storage to make use of the quantum attack-free characteristics of lattice- based cryptography. CPABSEL used the LWE hardness assumption to prevent quantum assaults. The authors introduced CP-ABSEL in cloud storage to make use of the quantum attack-free characteristics of lattice-based cryptography. The key computation section calculates patient key generation time. A block chain-based cypher text-policy attribute-based encryption system for cloud information sharing without trusting third parties. The use of blockchain- based ciphertext-policy attribute-based encryption helps to protect the rights of data owners. AES and weighted attribute- based encryption were used to safeguard data access. (AES- WABE). Reinforcement of concealment in cloud storage access policies is achieved by upgrading the CP-ABE method. The enhanced CP-ABE encrypted

data and employed logical connective operations to mask access policy attribute values. The authors utilized two types of attribute-based encryption, namely KP-ABE and CP-ABE, to implement fine-grained access control for patients' private medical data. Additionally, they incorporated blockchain technology to improve network efficiency for transmitting medical data and rapidly revoking access rights. MK-SABE is used to efficiently retrieve health records. A proposed solution for managing the growth of cloud-based personal health record (PHR) data is the implementation of authorized file-level de-duplication. Additionally, an efficient escrow-free CP-ABE system, known as EEF-CPABE, has been developed for secure storage of large amounts of data in the cloud. This system ensures constant size ciphertext and a secret key.

CSC-S lowers encryption and decryption calculation overhead in EEF-CPABE. The publication introduced a multi- user CP-ABE system with keyword search to let patients save their medical records and PHR data in medical clouds. AHRP algorithm provides secrecy, credibility, confidentiality and information access control. The security strategy for cloud storage, sharing, and retrieval of encrypted data relies on ABE. This approach enables access control for encrypted info and data retrieval through search access control. Suggests optimum attribute-based encryption (OABE). ABE seeks to improve public cloud data privacy. Beetle Swarm Optimization optimises crucial values for the ABE algorithm (BSO). The VMKS-ABE system. They enhanced the original ABE by introducing user revocation, secret key delegation, and ciphertext updating. This resulted in a new scheme called RS-HABE, which improves system security and meets application requirements. A patient-centric system paradigm for semi-honest server SHI access control. Authors have created an improved encryption technique, exceeding RSA, to encrypt the SHI files of patients. This method ensures fine- grained and scalable access control.

The author used a hybrid method to secure the hospital cloud database. First, AES is enhanced. The P-AES algorithm improves. RSA and P-AES form a hybrid algorithm. A new outsourced CP-ABE for cloud large data privacy and access control. Outsourcing encryption and decryption calculations to the proxy server minimises computing costs. Decentralized multi-authority CP-ABE access control is more practicable for user revocation. In the authors proposed an attribute-based cryptosystem and a block chain EHR system. ABE and IBE were used to encrypt medical data, while IBS was used to establish digital signatures. To protect cloud data, elliptic curve Diffie-Hellman for generation of secret key and identity attribute-based encryption were used. Employing the elliptic curve Diffie-Hellman method, the cloud user has the ability to seek medical information from the PHR admin and generate a secret. A secure cloud architecture employing modified CP- ABE and an attribute Bloom filter (ABF). They may conceal attributes and values in modified CP-ABE access controls.

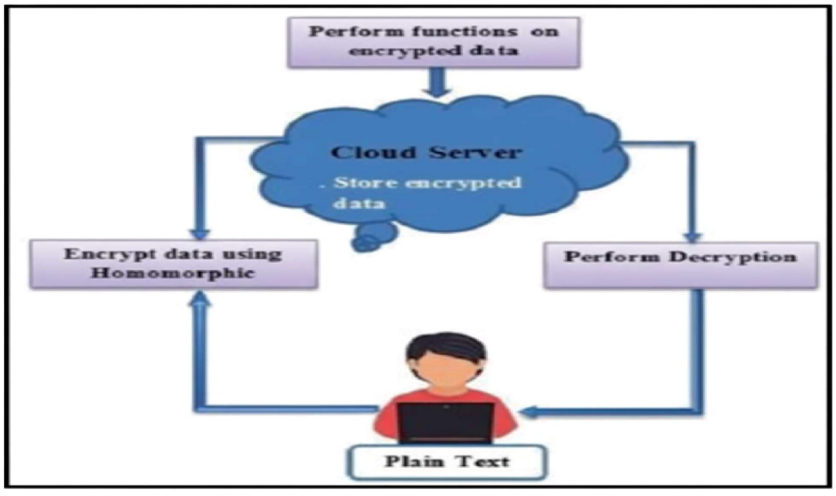

Fig 9 | Homomorphic encryption ensures the safety of data stored in the cloud

Homomorphic Encryption

Homomorphic Encryption technique permits calculations to be conducted on non-plain text, resulting in an encrypted result that matches the plain text result when decoded.[31] Numerous partly and completely homomorphic cryptosystems exist. FHE is safer than PHE. Figure 9 demonstrates the homomorphic encryption ensures the safety of data stored in the cloud. A Secure Partially Homomorphic Encryption (SPHE) technique secures outsourced data and performs multiplication and division on the cipher text. Cloud access control is more important. CTHE and MEHE were proposed[32] a hybrid cryptography-based AEDS for cloud data storage to increase data security and confidentiality without CTP intervention.

Nature-Inspired Algorithms

MSA and the enhanced blowfish algorithm enable safe data retrieval. MSA, data security, and data retrieval comprise the system. The blowfish algorithm (BFA) was proposed in] for cloud-based, security-aware information transmission. Pattern matching is used to identify the user and segregate imported data. The improved public cloud data integrity by using Qusai-adjusted levy fly distribution for the RSA cryptosystem (QMLFDRSA).

QMLFD for the RSA cryptosystem solves the public cloud data integrity challenge. Global mutation-based new artificial immune network optimization yields optimal key generation (GM-NAINO). Secure data transfer improves data integrity. [Algorithm. We start with the analogous node, build the transitional dataset, and perform the Opposition Cuckoo Search (OCS) method. Data integrity and privacy problems are addressed by CryptoGA.

For the security of cloud data, GA produces encryption and decryption keys using a cryptographic mechanism. The MKSVM classification technique is used to divide sensitive data into multiples. Encrypting segmented sensitive data using the best two-fish encryption technique. Cloud servers will request the best key. It is supported by a modified whale optimization

DOI: https://doi.org/10.70389/PJS.100206 | Premier Journal of Science 2025;15:100206

method (MWO). It used data distance. Blowfish encryption secures cloud data. The enhanced dragonfly algorithm improved accuracy. In, a hybrid encryption technique was combined with 2D-DWT-2 L or 2D-DWT-1 L steganography.

The hybrid encryption technique secures diagnostic data included in medical cover pictures using RGB channels by selectively using the AES and RSA algorithms. In, a fuzzy- based heuristic technique secures cloud storage allocation. This study clusters client systems using fuzzy rules. The lightweight HLE–SO method combines Paillier encryption with the KATAN algorithm. The suggested privacy preservation method includes data sanitization and restoration. The hybrid meta-heuristic algorithm generates the ideal key for the specified sanitization procedure. Jaya-based Shark Smell Optimization (JSO) is a hybrid approach that combines two effective strategies, SSO and JA (J-SSO). Introduces the Brainstorm-based Whale Optimization Algorithm (BS-WOA) for secret key identification. The data owner's database is updated using the optimum secret key to generate retrievable perturbation data for privacy and usefulness. Encrypts medical pictures using two-fold encryption. Blowfish encryption is evaluated first, followed by sign encryption to corroborate the encryption scheme. Opposition-based Flower Pollination (OFP) then upgrades private and public keys.

Concerns Regarding Data Storage's Safety and Confidentiality

Many firms provide cloud services. Since cloud servers are hacked, the CSP must protect consumers from data loss and security issues. Table 2. Shows the cloud security threats and countermeasures.

Availability

All cloud types private, public, communal, and hybrid face a major availability issue. Cloud computing availability provides services to consumers anytime, wherever virtual machines dominate infrastructure and platform CSPs. IP-blocking virtual machines are permitted here. For cloud system availability, these security techniques are paired alongside virtual machines.

Confidentiality

Cloud confidentiality means protecting user data. Cloud computing requires secrecy to manage user data across various data centres. Compared to the private network, the public network is facing significant problems due to the behavior of malicious cloud users. Thus, the CSP must carefully check malevolent users who saved DO data on the cloud server. To secure sensitive data, the CSP must maintain secrecy at many cloud application tiers.

Access Control

Access control restricts cloud server data to authorised users. The CSP monitors client and user data and file access requests via access control. Data access involves authentication, authorization, and responsibility. Dos must constantly be online for cloud computing data access. Access is impossible without DOs online. CSPs sometimes scan the whole database for one data. Thus, searching costs grow and cloud server data retrieval takes longer. Cloud computing raises data security risks. Government database surveillance might initially pose several hazards. Data may be stored anywhere in the cloud. It belongs to that country's government. Foreign governments without notice may access customer data. Second, approved IT company users provide criminal users with their databases. Malicious individuals may then access cloud server data. Many cloud workers violate security standards.

Data Related Issues

There are various data-related difficulties, which are listed below:

Data integrity in the cloud prevents unauthorised users and CSPs from altering user data. Sometimes DO data differs from user data. Hackers alter data. The CSP must ensure user data integrity.

- **Data loss:** The cancellation of services by the cloud provider may occur due to a financial crisis or other factors. The inability of users to access data at a later time is attributed to the lack of storage on cloud servers. Data loss is a common occurrence in cloud computing.
- **Data leakage:** hackers or malevolent users steal data. Hackers constantly steal original data and private information always a major concern.
- Users are unaware of the location of data. Users are not able to see the data. It may be kept abroad or at home. The CSP stores data. Most CSPs have global datacenters.
- **Unwanted access:** Cloud computing poses various hazards to data and file confidentiality. If user data is

Table 2 | Cloud security threats and countermeasures

Threat Category	Examples	Countermeasures Discussed in Literature (2017–2022)
Availability	Service downtime, VM blocking, DoS	Redundant storage, load balancing, IP blocking, VM isolation
Confidentiality	Unauthorized access, malicious insiders	Data encryption (AES, RSA, IBE, ABE), secure key management
Integrity	Data tampering, corruption	Hashing, digital signatures, blockchain-based logging
Data Loss & Leakage	Accidental deletion, CSP shutdown, theft	Backup strategies, data fragmentation, escrow-free ABE
Access Control	Unauthorized file retrieval	Role-based access, attribute-based encryption, audit mechanisms
Vendor Lock-in	Dependence on single CSP	Multi-cloud strategies, data portability standards
Audit & Compliance	Lack of transparency, legal issues	Third-party audits, compliance frameworks, logging mechanisms

held outside their nation, the government of that country may examine it. As a result, user data is at risk.

- **Data segregation:** Cloud users share storage devices. The CSP does not save device-specific user data. Missegregation of data steadily increases the risk. Isolating client data on the cloud server solves this issue. Today, encryption solves this. Strong encryption may raise expenses. Encryption destroys data. CSPs may encrypt data. The CSP must remember that encryption must not destroy or affect user data.
- **Seller lock-in:** This strategy makes consumers reliant on the vendor. IT solutions lock in vendors. Cloud computing is a significant issue. If a vendor stops offering a service, the CSP will try to get it from another vendor, maybe another cloud server. Switching CSPs is complicated and risky.
- **Data deletion:** A significant issue with cloud servers is determining if data or files have been permanently deleted. CSPs backup all cloud server data. There is no way to verify that cloud server data is erased. Multiple devices hold CSP data. The cloud server cannot delete a device with a lot of data. Thus, DOs face severe data issues.
- **Analysis:** Cloud computing has many distributed systems. Thus, finding information is hard. The CSP analyses data requests slowly. Giving information takes longer. The CSP stores data in several data centres over a large region, complicating the situation.
- **Secure data transfer:** Cloud computing involves communication between consumers and cloud providers. Attackers may simply exploit cloud data if they have a connection. A cloud system without a secure data connection route might cause serious issues for clients. The CSP must secure data transfers.
- Customer data can be manipulated through various methods like cross-site scripting, command injection, unsafe direct object references, SQL injection, and others. Web apps are hacked by hackers.

Storage Related Issues

Cloud computing lets CSPs or third parties store and manage data on their servers. Remote drives store data. CSP data storage is massive. Storage costs money.

- **Users access:** CSP services through an internet API. Data safety is ensured through CSP data fragmentation. After splitting, the CSP stores data in many data centres. Data may be retrieved from a crashed part. Below are many data storage issues:
- **Protector:** Users worry about resource risk since the CSP controls all cloud tasks and is untrusted. Cloud providers must be more aware.
- **Ownership:** Some users worry about losing ownership of cloud data after a long period. Strong agreements solve this issue for many CSPs. These agreements guarantee data rights for users.
- **Multiplatform support:** IT departments must integrate cloud services with Linux, OS, Windows, and others. IT firms employing cloud services need multiplatform support.
- **Data recovery:** Cloud server accidents happen. Data may be lost. The CSP backs up data for recovery.
- **Data portability and conversion:** In crucial situations, data transmission is challenging. The CSP partitions and converts files. After converting, the CSP must remember data format, which malicious users cannot see.

Security Issues

Traditional cloud management had self-control. Cloud security is critical because users may store private data or files outside their domain.[33] Public clouds present privacy and security problems. A new poll ranks cloud security as the biggest issue. In cloud computing, determining security responsibility is the fundamental concern. No API standard causes this security problem. The cloud security alliance lists unsecured interfaces, data loss, account hijacking, malevolent insiders, shared technology difficulties, or leakage, and an unclear risk profile as the key cloud computing risks.

- **Identity Verification:** CSPs authenticate and offer services using Identity Management (IDM). IDM interoperability is an issue. IDM has multiple identity tokens and identity negotiation techniques. Passwords restrict authentication methods. IDM systems must safeguard users and process data. IDM is unclear with multi-tenant cloud servers. A multi-tenant cloud architecture must separate customer data.
- **Backup:** Cloud computing makes availability and backup challenging. Failures need data backup. Users are seldom informed about CSP backup files. Self-optimization and self- healing are new cloud hazards. Business continuity and data backup are ensured through self-healing. The fundamental issue is that data processing is untraceable. Self-optimization involves decision-making autonomy. The CSP self-optimizes to meet user needs. The most serious concerns stem from a lack of cloud computing standards. Standardization prevented virtual enterprises from adopting grid computing. Service-Oriented Architecture (SOA) sought to improve standards to fix various problems. CSPs, DOs, and users communicate differently in cloud computing. Lack of standards affects security framing in diverse contexts.
- **Multi-tenancy:** A SAAS server runs one programme that several enterprises employ. This programme partitions data virtually. Other organisations may utilise the software part. Job scheduling algorithms help CSPs optimise hardware usage. Most CSPs virtualize to maximise hardware consumption. VMs are separated, making hardware sharing safe. Virtualization introduces cross-VM side-channel attacks.
- **Audit:** CC CSPs must oversee implementation. CSPs need external audits. Cloud computing audit concerns are growing. Data integrity requires cloud server transaction records. The public cloud has yet to complete a comprehensive audit.

DOI: https://doi.org/10.70389/PJS.100206 | Premier Journal of Science 2025;15:100206

Possibly Forthcoming Change Regarding the Cloud Computing Security Issue

For the aforementioned issues, we believe there will be two potential research methods.

- To enhance privacy protection, it is crucial to establish an extensive framework that effectively conceals sensitive information within shared data. This is particularly crucial for data that contains very sensitive information, such as information from social networking sites, the government, or medical records.
- Conceive of an effective optimization strategy to enable a greater number of encryption algorithms for optimum key generation and safe data storage in the cloud.

Quantum Cryptography for the Purpose of Database Encryption in the Cloud

- Quantum cryptography improves large-data security, database management, and simplicity. For large data security, the symmetric key for a cypher text must be retrieved. Quantum Key Distribution (QKD) has gained technological attention since quantum cryptography's discovery. QKD uses quantum characteristics to exchange sensitive data like secret keys needed to encrypt data before storing it on the cloud service provider's database. QKD security relies on unbreakable rules to boost quantum computer computing capability. QKD is ideal for conventional encryption and constructing secure regions for massive security or quantum computing. QKD protects against eavesdropping. The principles of quantum mechanics are applied in QKD.
- A free-space quantum channel to transport light states between Alice and the receiver (Bob). This channel doesn't require security.
- A public but verified communication channel from both sides for post-processing and a proper and secret key.
- A key exchange protocol that exploits features to discover eavesdroppers or issues by analysing intercepted data.

Future Directions

Based on the reviewed literature in the PDF, future research should focus on (1) post-quantum cryptography tailored for cloud storage, (2) optimization of encryption through AI/nature-inspired algorithms, (3) revocation-friendly fine-grained access control, (4) blockchain-integrated secure sharing, (5) practical privacy-preserving computation, and (6) secure multi-cloud portability frameworks. These directions move beyond enumeration and directly address the gaps identified in the manuscript.

Conclusion

Cloud computing and data protection are difficult. This is addressed in a number of works. The current investigation into a solution is insufficient. This research examined the best methods for safely sharing data in the cloud and data protection. The necessary and sufficient information needed to understand the method's core and each solution's future is underlined. The cited approaches are also analysed and compared. Every approach is assessed for context.

References

1 Prabu Kanna G, Vasudevan V. A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data. Cluster Comput. 2019;22(4):9561–9.
2 Daniel E, Vasanthi NA. LDAP: a lightweight deduplication and auditing protocol for secure data storage in cloud environment. Cluster Comput. 2019;22(1):1247–58.
3 Shanmugapriya E, Kavitha R. Medical big data analysis: preserving security and privacy with hybrid cloud technology. Soft Comput. 2019;23(8):2585–96.
4 Masud M, Gaba GS, Choudhary K, Alroobaea R, Hossain MS. A robust and lightweight secure access scheme for cloud based E-healthcare services. Peer-to-Peer Netw Appl. 2021;14(5):3043–57.
5 Thabit F, Alhomdy S, Jagtap S. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. Int J Intell Netw. 2021;2:18–33.
6 Qiu H, Noura H, Qiu M, Ming Z, Memmi G. A user-centric data protection method for cloud storage based on invertible DWT. IEEE Trans Cloud Comput. 2019;9(4):1293–304.
7 Namasudra S, Devi D, Kadry S, Sundarasekar R, Shanthini A. Towards DNA based data security in the cloud computing environment. Comput Commun. 2020;151:539–47.
8 Joseph T, Kalaiselvan SA, Aswathy SU, Radhakrishnan R, Shamna AR. A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. J Ambient Intell Humaniz Comput. 2021;12(6):6141–9.
9 Hu X, Wei L, Chen W, Chen Q, Guo Y. Color image encryption algorithm based on dynamic chaos and matrix convolution. IEEE Access. 2020;8:12452–66.
10 Kakkad V, Patel M, Shah M. Biometric authentication and image encryption for image security in cloud framework. Multiscale Multidiscip Model Exp Des. 2019;2(4):233–48.
11 Stergiou C, Psannis KE. Efficient and secure big data delivery in cloud computing. Multimed Tools Appl. 2017;76(21):22803–22.
12 Shankar A, Pandiaraja P, Sumathi K, Stephan T, Sharma P. Privacy preserving E-voting cloud system based on ID based encryption. Peer-to-Peer Netw Appl. 2021;14(4):2399–409.
13 Tahir S, Ruj S, Rahulamathavan Y, Rajarajan M, Glackin C. A new secure and lightweight searchable encryption scheme over encrypted cloud data. IEEE Trans Emerg Top Comput. 2017;7(4):530–44.
14 Deng H, Qin Z, Wu Q, Guan Z, Deng RH, et al. Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Trans Inf Forensics Secur. 2020;15:3168–80.
15 Qin J, Li H, Xiang X, Tan Y, Pan W, et al. An encrypted image retrieval method based on Harris corner optimization and LSH in cloud computing. IEEE Access. 2019;7:24626–33.
16 Namasudra S, Chakraborty R, Majumder A, Moparthi NR. Securing multimedia by using DNA-based encryption in the cloud computing environment. ACM Trans Multimed Comput Commun Appl. 2020;16(3s):1–19.
17 Morales-Sandoval M, Gonzalez-Compean JL, Diaz-Perez A, Sosa-Sosa VJ. A pairing-based cryptographic approach for data security in the cloud. Int J Inf Secur. 2018;17(4):441–61.
18 Deepa N, Pandiaraja P. E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption. J Ambient Intell Humaniz Comput. 2021;12(5):4877–87.
19 Jemihin ZB, Tan SF, Chung GC. Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey. Cryptography. 2022;6(3):40.
20 Asif R. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. IoT. 2021;2(1):71–91.
21 Nauman Khan M, Rao A, Camtepe S, Pieprzyk J. Classical to Post-Quantum Secure ABE-IBE Proxy Re-Encryption Scheme. In: Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT); 2023.
22 National Institute of Standards and Technology. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. Gaithersburg (MD): NIST; 2024 Aug 13 [cited 2025 Dec 22]. Available from: https://

www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
23 National Institute of Standards and Technology. Transition to Post-Quantum Cryptography (Initial Public Draft). Gaithersburg (MD): NIST; 2024 Nov 12. Report No.: NIST IR 8547.
24 Alvarado M, Gayler L, Seals A, Wang T, Hou T. A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges. arXiv [Preprint]. 2023 [cited 2025 Dec 22]: [22 p.]. Available from: https://arxiv.org/abs/2312.10430
25 Cintas Canto A, Kaur J, Mozaffari Kermani M, Azarderakhsh R. Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security. arXiv [Preprint]. 2023 [cited 2025 Dec 22]: [34 p.]. Available from: https://arxiv.org/abs/2305.13544
26 Chowdhury S, Covic A, Acharya RY, Dupee S, Ganji F, Forte D. Physical Security in the Post-Quantum Era: A Survey on Side-Channel Analysis, Random Number Generators, and PUFs. arXiv [Preprint]. 2020 [cited 2025 Dec 22]: [25 p.]. Available from: https://arxiv.org/abs/2005.04344
27 Huang B, Gao J, Li X. Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing. J Cloud Comput (Heidelb). 2023;12(1):37.
28 Bhoi SS, Arakala A, Corman AB, Rao A. Post-Quantum Homomorphic Encryption: A Case for Code-Based Alternatives. Cryptography. 2025;9(2):31. https://doi.org/10.3390/cryptography9020031
29 Yao Y, Chen H, Shen L, Wang K, Wang Q. A CP-ABE Scheme Based on Lattice LWE and Its Security Analysis. Appl Sci. 2023;13(14):8043. https://doi.org/10.3390/app13148043
30 Hou J, Peng C, Tan W, Ding H. Quantum-Resistant Multi-Feature Attribute-Based Proxy Re-Encryption Scheme for Cloud Services. CMES-Comput Model Eng Sci. 2023;138(1):917–38. https://doi.org/10.32604/cmes.2023.027276.
31 Savadatti S, Cherukuri AK, Jonnalagadda A, et al. Analysis of quantum fully homomorphic encryption schemes (QFHE) and hierarchial memory management for QFHE. Complex Intell Syst. 2025;11:264. https://doi.org/10.1007/s40747-025-01851-7
32 PrabhuKavin B, Ganapathy S, Kanimozhi U, Kannan A. An enhanced security framework for secured data storage and communications in cloud using ECC, access control and LDSA. Wirel Pers Commun. 2020;115(2):1107–35.
33 Kumar S, Srivastava PK, Srivastava GK, Singhal P, Singh D, Goyal D. Chaos based image encryption security in cloud computing. J Discrete Math Sci Cryptogr. 2022;25(4):1041–51.