Computer Fraud and Security
ISSN (online): 1873-7056

# Security and Privacy-Preserving Data Sharing Mechanisms for Cloud-based Personal Health Records: A Systematic and Comparative Review

**[*1]Naveen John J, [2] Dr.I. Shatheesh Sam**
[*1]Department of Computer Science, Nesamony Memorial Christian College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli, India.
[2]Associate Professor in the Department of PG Computer Science, Nesamony Memorial Christian College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli, India.
[*1]Corresponding Author Email: naveenjohnmano@gmail.com

**Abstract**
Cloud computing has become a prominent platform for storing and sharing Personal Health Records (PHRs) due to its scalability and cost efficiency. However, outsourcing sensitive medical data introduces security challenges such as unauthorized access, data breaches, and complex key management. This paper presents a systematic review of secure data sharing mechanisms for cloud-based PHR systems published between 2016 and 2026. A total of 70 peer-reviewed articles were analyzed and categorized into cryptography-based approaches, blockchain frameworks, authentication mechanisms, AI-integrated models, and hybrid architectures. The findings reveal that attribute-based encryption and blockchain technologies are widely adopted to enhance confidentiality and access control, while recent studies emphasize AI-driven and federated learning-based security solutions. Despite advancements, issues related to computational overhead, scalability, and key management persist. This review identifies existing research gaps and highlights future directions toward lightweight encryption and adaptive healthcare security frameworks.

**Keywords:** Cloud computing, Personal Health Record (PHR), Data privacy, Data Sharing, Security, AI-Integrated.

## 1. INTRODUCTION

A Personal Health Record (PHR) is a type of electronic system employing a person to record, manage, and share health details securely. PHRs have been designated as a national priority by several governments in the United States, comprising the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare and Medicaid Services (CMS) (Khan et al., 2020). Unlike Electronic Medical Records (EMRs), which are held at an individual healthcare provider's facility, Electronic Health Records (EHRs) allow for interoperability between facilities (e.g., hospitals, doctors' offices, etc.). PHR systems, however, focus on the patient and are designed to integrate many types of health data obtained from a variety of sources, devices, and networks, to assist individuals in preventing illness, self-managing their health care, and providing long-term management of disease (Kusunose and Muto 2023; Lee 2020). In general, there are three categories of PHR systems: (i) stand-alone PHR systems that allow patients to manually create their own record; (ii) tethered PHR systems that connect to the EMR system of a healthcare provider or health insurance company; and (iii) integrated PHR systems that use cloud-based health information exchange (HIE) platforms to link together care from multiple provider organizations (Hosseini et al., 2023). Cloud-based PHR systems provide scalability, ubiquity, and elasticity while enabling patients to control access permissions, facilitate secure medical information sharing, and enhance healthcare quality and collaboration (Hosseini et al., 2023). Figure 1 shows the PHRs in cloud storage refer to the digital management of patient health information on remote cloud infrastructures rather than local healthcare servers.

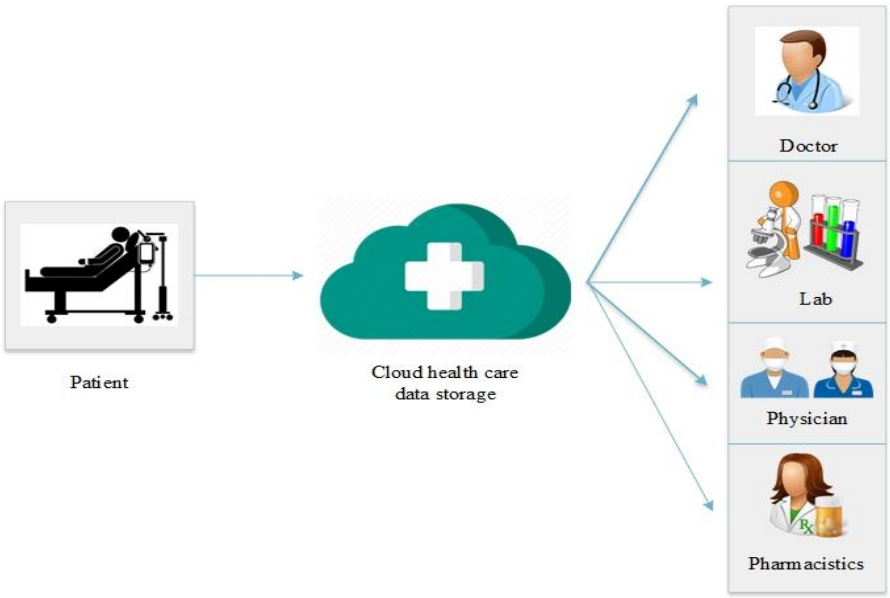


**Figure.1 PHR in Cloud Storage**

Cloud computing acts as the backbone for storing a huge amount of patient health records on a remote server, which can be accessed through the internet from anywhere. This ability facilitates effective data sharing and collaboration among health care systems (Wu and Liu 2025; Kuppuswamy et al., 2020). Cloud-based PHR systems can store very sensitive medical data, which raises serious concerns about protecting patient information from unauthorized access. Among the biggest obstacles facing cloud computing is how to protect patient data from cyber-attacks because of the open as well as dispersed nature of the cloud, and how to ensure that all individuals who have different access privileges have robust mechanisms, due to the nature of the cloud, to provide access to authorized individuals but to deny unauthorized individuals from accessing patient data (Liu). Cloud computing, through three models of service delivery (IaaS, PaaS, and SaaS), allows for different levels of control and management (Putzier et al., 2024) to improve the availability of patient data and to alleviate some of the burdens of managing an organization's infrastructure; however, even with private cloud models like ownCloud (Kumar et al., 2024), concerns about ensuring confidentiality, integrity and secure outsourcing are still prevalent.

Cloud security plays a fundamental role in protecting data, applications, and computing resources across public, private, and hybrid cloud environments (Dawood et al., 2023). In medical care, the safe transfer of highly confidential information from researchers to hospitals or health insurers, among other institutions, is vital for improving the standards of treatment for patients and enhancing medical research (Ahammed et al., 2024). Nevertheless, maintaining a balance between efficient data sharing and privacy is no small feat. In addition to this, new AI technologies increase this problem, as AI health care systems depend on vast amounts of patient data for learning and analysis purposes. To mitigate the risks associated with maintaining patient confidentiality, several privacy-preserving techniques (PPTs) have been implemented, including secure multi-party computation, federated learning with secure aggregation, differential privacy, homomorphic encryption and trusted execution environments (Shree et al., 2024). Despite these advancements, existing approaches often significant computational costs, limited scalability and complex key management with insufficient real-world testing (Shakor et al., 2024; Shakor et al., 2024; Chakilam et al., 2025). Additionally, most studies provide only isolated solutions for PHR data sharing instead of composite views of secure sharing of PHR data. Therefore, a thorough analysis of the existing mechanisms used to share PHR data is needed to identify research gaps and to help create future directions for the creation of secure, scalable and privacy-aware cloud-based PHR systems.

## 2. RESEARCH METHODOLOGY

This investigation uses a methodical review of the literature to examine secure data sharing mechanisms in cloud-based Personal Health Record (PHR) networks. The review analyses national and international research on how encryption techniques, blockchain models, authentication mechanisms, and privacy-preserving approaches are designed and implemented to protect sensitive healthcare data in cloud environments. The studies that are relevant to the subject matter and have been published from 2016 to 2026 in the peer-reviewed scientific databases are selected for evaluation. Every

chosen paper will be assessed on the grounds of the quality of methodology adopted, its relevance to the security of PHRs, its analysis of performance, scalability, and its practicality.

### 2.1 Databases Searched

Data sources used to conduct this review involved the large scientific databases such as IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and PubMed, along with Google Scholar, which allowed identifying additional sources of literature on the issue under discussion. The searches involved only peer-reviewed academic journal articles and high-quality conference papers concerning cloud computing, PHR security, blockchain implementation in the healthcare industry, encryption methods, and privacy solutions. The use of several databases when looking for literature offered an opportunity to find complete coverage of theoretical and practical literature on the security and privacy of information stored in cloud PHRs.

### 2.2 Keywords Used

The databases used to gather information for the review were: IEEE Xplore, Scopus, ScienceDirect, Springer Link, PubMed, and Google Scholar. The searches conducted involved the use of keywords associated with cloud-based PHRs, security methods for PHRs, encryption methods, blockchain-based PHRs, and privacy-preserving techniques for PHRs. Examples of such combinations include: “PHR AND Cloud Security”, “Personal Health Record AND Blockchain”, “Attribute-Based Encryption AND Healthcare”, “Secure Data Sharing AND Cloud Healthcare”, and “Privacy Preserving Techniques AND Medical Data.”

Through the use of these terms, it was possible to conduct the systematic search of peer-reviewed journal articles and top-notch conference papers containing information on secure PHR data sharing, access control systems for PHRs, PHR data authentication processes, and PHR data scalability challenges in cloud computing environments. Through this search methodology, it became possible not only to identify the gaps in the current scientific literature on cloud-based PHR data security but also to conduct a detailed analysis of PHR data technologies in the cloud computing environment. Table 3.1 presents the databases and search terms used to retrieve data for this review.

**Table.1 Databases and Search Strings Used**

| Database | Search Strings / Keywords Used |
|---|---|
| IEEE Xplore | • Personal Health Record AND Cloud Security • Secure Data Sharing AND Healthcare Cloud • Attribute-Based Encryption AND PHR • Blockchain AND Healthcare Security |
| Scopus | • Cloud-based PHR AND Privacy • Access Control AND Medical Data • Secure Authentication AND Healthcare Cloud |
| ScienceDirect | • Privacy-Preserving Techniques AND Healthcare • Homomorphic Encryption AND Medical Data • Federated Learning AND Health Records |
| SpringerLink | • Blockchain-based PHR Systems • Cryptography AND Cloud Healthcare • IoT Healthcare AND Security |
| PubMed | • Electronic Health Records AND Data Security • Patient Data Privacy AND Cloud Computing |
| Google Scholar | • Secure PHR in Cloud Computing • AI AND Healthcare Data Privacy • Access Control Models in Healthcare Systems |

### 2.3 Inclusion Criteria

The articles this study reviewed were comprised of high-quality peer-reviewed journal articles and conference papers published between 2016 and 2026 in the English language and available as full-text. The focus of the articles was on security and privacy mechanisms for cloud-based Personal Health Record (PHR) systems or systems that share healthcare data. Studies dealing with cryptographic algorithms, blockchain architecture, authentication mechanisms, access control, and privacy protection technologies were considered. Thus, both theoretical and empirical studies that provided some technical contributions were considered.

### 2.4 Exclusion Criteria

Articles that are non-peer reviewed, editorial pieces, workshop papers, unpublished articles, and studies that do not have access to their full text were all excluded in this literature review. Studies that are not associated with health care systems or PHR systems and those that did not involve cloud security in terms of medicine were also excluded. Any studies that

did not have enough technical details, validation, or performance evaluation to establish a level of quality or relevance to the review were excluded from this review.

### 2.5 Study Selection and Analysis

To guarantee the inclusion of excellent and pertinent research articles about secure cloud-based Personal Health Record (PHR) systems, a methodical study selection process was carried out. Primarily, performed a thorough initial search of the major academic databases (IEEE Xplore, Scopus, ScienceDirect, SpringerLink, etc.) for relevant articles using predefined keywords covering such concepts as PHR security in the cloud, Attribute-Based Encryption (ABE) for healthcare, Blockchain security for healthcare, AI security for healthcare, and secure cloud data sharing. To use the following criteria as the basis for making our inclusion decisions: (1) Peer-reviewed journal and conference articles; (2) Articles published between 2016 and 2026; (3) Articles related to the security, privacy, authentication, encryption, blockchain or AI-related mechanisms associated with PHR/EHR systems; and (4) Articles written in English. We used the following criteria as a basis for exclusion from the analysis: duplicate records; articles published in non-peer-reviewed journals; short abstracts without full text; irrelevant cloud-based studies; purely clinical studies performed without collecting security information. After removing duplicates and screening titles and abstracts, the full texts of the remaining articles were carefully reviewed to assess relevance and methodological quality. A total of 70 articles were selected for detailed analysis. The selected studies were categorized into five major groups: cryptography-based approaches, blockchain-based frameworks, authentication and session key mechanisms, AI-integrated security models, and hybrid architectures. Figure 2 illustrates the PRISMA-based study selection process adopted in this review.

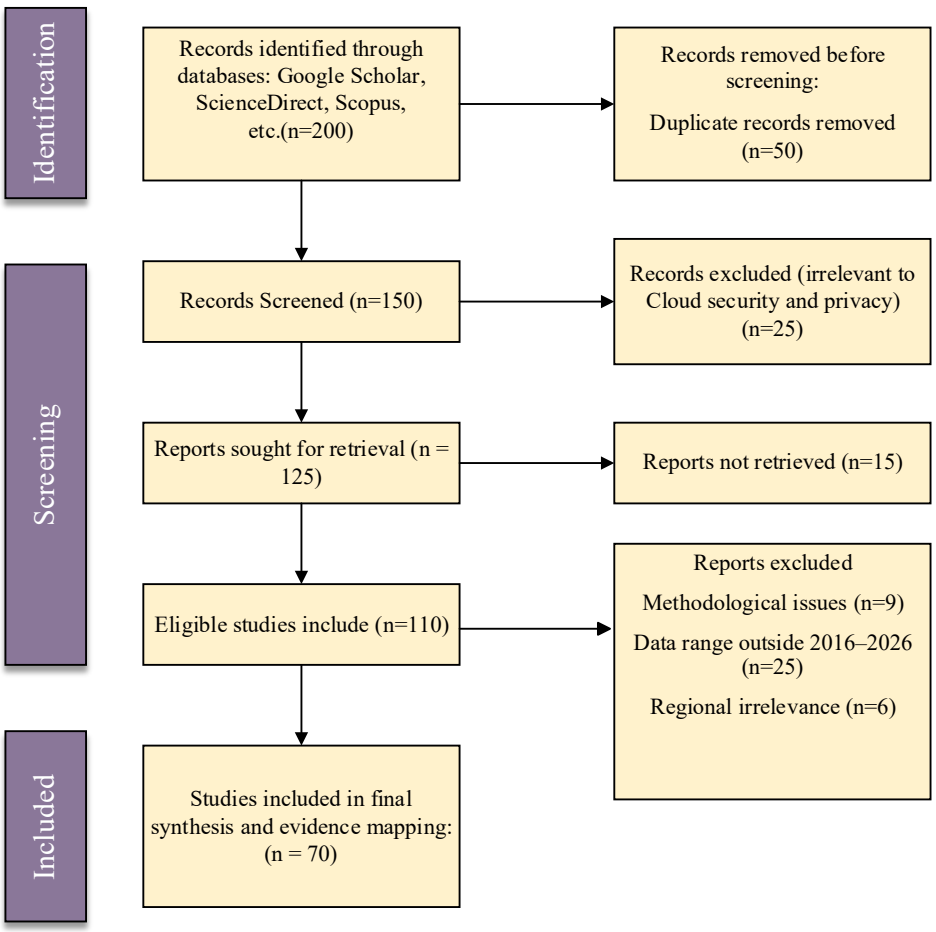


**Figure.2 PRISMA Flow Diagram of Study Selection Process**

## 3. TAXONOMY OF SECURE PHR DATA SHARING APPROACHES

### 3.1 Cryptography-Based Approaches

Cryptography-based techniques represent the backbone that underlies cloud-based PHR/EHR security solutions. They make use of state-of-the-art encryption algorithms to ensure confidentiality, integrity, granular access control, and secure data exchange in a distributed medical setting. Figure 3 presents an architectural representation of a cryptography-based PHR security solution running in a cloud environment.

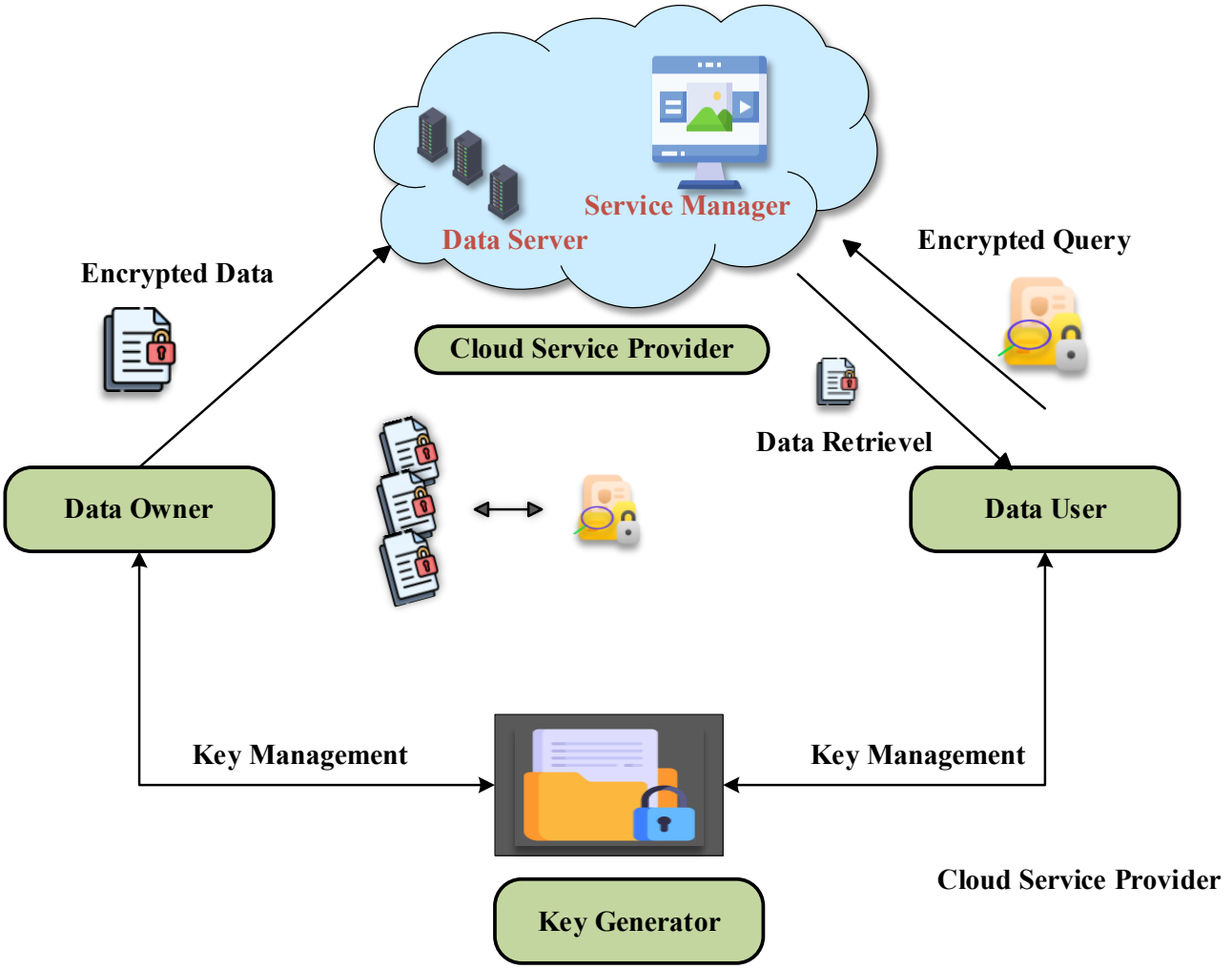


**Figure.3 Architecture of a Cryptography-Based Secure Cloud PHR System**

Walid et al., 2024 conducted a detailed analysis of various types of ABE schemes such as Ciphertext Policy ABE (CP-ABE), Key Policy ABE (KP-ABE), and Multi-Authority ABE (MA-ABE), in the healthcare industry. In their research, they used the MIMIC-III database and knowledge graph-based EHR systems to examine the encryption process at different record sizes. Their findings showed performance variations and scalability comparisons between ABE schemes, but they pointed out that there is no standard for benchmarking in healthcare applications.

Rodrigues et al., 2023 proposed an approach towards sharing patients' data with a focus on empowering patients to manage their medical records. The framework utilizes a proxy re-encryption scheme that allows patients to give or withdraw access rights to third parties regarding their health information. Also included a break-glass feature for emergency access through a centralized trusted entity. Performance evaluation demonstrated the feasibility of PRE in enhancing controlled and secure data delegation; however, reliance on a trusted authority introduces partial centralization concerns.

Das et al., 2022 proposed an elliptic curve cryptography (ECC) based CP-ABE model for resource-constrained IoT healthcare environments to address the high complexity of the traditional CP-ABE scheme. the proposed scheme reduces encryption/decryption time because it replaces bilinear pairing operations with ECC mechanisms. The proposed model improves scalability and reduces the computational burden on end-users by allowing for multiple attribute authorities and

outsourced decryption. Formal security proofs and performance evaluations show that the ECC based CP-ABE model is more efficient than traditional CP-ABE implementations.

Saravanan et al., 2021 proposed a HAP-CP-ABE framework to provide secure cloud-based personal health record (PHR) systems through the combination of hash-based authentication and CP-ABE encryption. The model uses three phases: authentication phase, secure upload phase, and secure download phase. The process involves extract features from the data using the ENT-LDA approach, creating a hash-based authentication password (HAP) using SHA 512, and then encypting the data with CP-ABE to provide access to the records after verification of the user's HAP.

Hindhuja et al., 2025 established a Proxy Re-Encryption (PRE)-based framework for secure cloud data sharing, enables secure sharing of cloud data using data that has been segmented into blocks and hashed for integrity using SHA before encrypting each block. A proxy server performs encryption through the use of previously encrypted data allowing a legitimate user to decrypt records using their designated decryption key. The integration of Attribute Based Encryption (ABE), Role Based Access Control (RBAC), and efficient delegation of keys makes possible for flexible and scalable access control options while also ensuring the protection of confidential information as well as preserving the owner's sovereignty over the data.

Ramesh et al., 2026 proposed the Secure Data–Monarch Butterfly Optimization Algorithm (SD-MBOA) to improve the efficiency of Attribute-Based Encryption in cloud environments. Using meta-heuristic optimization, resulting in an overall decrease in both the time taken to perform encryption and decryption operations on large datasets compared to traditional methods. The experimental results of the SD-MBOA demonstrate that it has significantly improved the resource management performance of an application's compute resources thus making it an ideal candidate for cloud-based healthcare applications with scalable access to compute resources through their architecture.

Sourav, and Rifaqat Ali 2024 introduced a new lattice-based ring signcryption scheme called LRS-SHM specifically to provide quantum resistant security for managing healthcare data. The framework utilizes regenerated user-controlled keys along with a (t,n) threshold secret sharing mechanism which serves to eliminate any single point of failure as well as promote user anonymity. A formal security analysis performed under the random oracle model showed both confidentiality and nonforgeability will be upheld with this method, while also providing improved resilience to attacks made by quantum sources and maintaining the efficient key management process already established.

Wang et al., 2026 proposed a decentralized MA-ABE (Multi-Authority Attribute-Based Encryption) system to meet the challenges of privacy and efficiency in cloud-based healthcare systems. Current MA-ABE systems result in long ciphertexts and have high computational overhead. Wang et al.'s approach eliminated the need for a central authority and could generate shorter ciphertexts, improving the efficiency of encryption and decryption operations. The results of experiments conducted with the Pairing-Based Cryptography library were consistent with and demonstrated improvements to performance and less computational burden compared to current systems.

Chen et al., 2023 suggested a BPVSE (Blockchain-Enabled Verifiable and Dynamic Searchable Encryption) for cloud-assisted Electronic Health Record (EHR) systems by implementing a combination of blockchain and hash proof chain technologies to allow for public verification of search results without the need for a trusted third party. BPVSE supports dynamic updates to the data, provides forward and backward security for data updates, and allows for multiple search processes to be performed simultaneously on the same data. BPVSE has been formally proven to provide improved functionality, security, and efficiency compared to similar efforts.

Ali et al., 2025 introduced a multi-authority CP-ABKS proposal to resolve single point failure issues and key distribution concerns that exist within EHR systems in the cloud. Their TMABKS framework employs an anonymous key mechanism with oblivious transfer protocols for both expected key distribution of attributes in a secure manner as well as protecting the privacy of the attribute distribution.

Exceline et al., 2022 proposed biometric-based multi-authority Ciphertext-Policy Inner Product Encryption (CP-IPE) method to improve the data protection, privacy, and segmented access control of medical documents (EHR) in a Cloud Environment. The use of elliptic curve cryptography (ECC) and the access structure of access control integrated into ciphertext increases confidentiality while reducing users' complexity of being denied access. Table 2 presents the comparative analysis of cryptography-based approaches for secure cloud-based healthcare systems.

**Table.2 Cryptographic Techniques for Secure Healthcare Cloud Systems**

| Authors | Core Technique | Key Contribution | Strengths | Limitations |
|---|---|---|---|---|
| Walid et al. | CP-ABE, KP-ABE, MA-ABE | Comparative evaluation of major ABE variants using MIMIC-III dataset | Identifies scalability & performance trade-offs; practical benchmarking | Lack of standardized healthcare benchmarking framework |
| Rodrigues et al. | Proxy Re-Encryption (PRE) | Patient-centric access control with dynamic delegation & break-glass mechanism | Flexible access grant/revocation; emergency access support | Reliance on trusted authority (partial centralization) |
| Das et al. | ECC-based CP-ABE | Replaces bilinear pairing with ECC for IoT healthcare | Reduced encryption/decryption time; scalable for resource-constrained devices | Limited validation on large-scale real-world datasets |
| Saravanan et al. | HAP-CP-ABE | Hash-based authentication + CP-ABE encryption | Strong authentication; secure upload/download phases | Additional feature extraction overhead |
| Hindhuja et al. | PRE + ABE + RBAC | Secure segmented data sharing with SHA integrity verification | Flexible access control; preserves data owner sovereignty | Increased system complexity |
| Ramesh et al. | SD-MBOA optimized ABE | Meta-heuristic optimization for faster ABE operations | Reduced encryption/decryption time for large files | Added algorithmic computation overhead |
| Sourav & Rifaqat Ali | Lattice-based Ring Signcryption (LRS-SHM) | Quantum-resistant healthcare data protection with (t,n) threshold scheme | Quantum security; eliminates single-point failure; strong anonymity | Higher implementation complexity |
| Wang et al. | Decentralized MA-ABE | Short ciphertext & removal of central authority | Improved efficiency; reduced computational burden | Still dependent on pairing-based cryptography |
| Chen et al. | BPVSE (Blockchain + Searchable Encryption) | Public verifiable dynamic search over EHR | Forward/backward security; no trusted authority | Blockchain overhead |
| Ali et al. | TMABKS (Multi-Authority CP-ABKS) | Anonymous key distribution via Oblivious Transfer | Secure keyword search; traceability; dynamic revocation | Increased key management complexity |
| Exceline et al. | Biometric-based Multi-Authority CP-IPE | Hidden access structure with ECC | Enhanced privacy; reduced access rejection complexity | Requires biometric infrastructure |

### 3.2 Blockchain-Based Approaches

The use of blockchain technology to improve security, trust, and transparency in cloud PHR and EHR systems has shown promise as a potential solution. With the application of blockchain technology, such systems remove single-point failures and maintain data integrity, accountability, and immutability. Emerging research in the area has concentrated on patient-controlled access, verifiable access control, and secure data sharing. Patient-controlled blockchain access control systems provide users with the ability to set their own consent conditions when it comes to access by medical service providers.

Dong et al., 2023 developed a blockchain-based PHR sharing system enables insurance companies to share the patient's health record in a way that is under the patient's control and secure through the patient's own consent management system. The prototype consists of a blockchain-enabled access-control (BAC) model built upon the Hyperledger Fabric development framework with the capability for the sharing parties to mutually validate access to the patient's record through a consensus method based on the blockchain network.

Costa et al., 2022 proposed a Blockchain-enabled Distributed Ledger Architecture for enabling secure, standardized, and interoperable PHR management on a permissioned distributed network using the Hyperledger Fabric development framework. and evaluated using Hyperledger Caliper, the system was assessed under varying workloads (100–2500 simultaneous submissions) and network sizes (3–13 peers). Results showed that read operations achieved higher throughput than write operations, while increased network size reduced write throughput and increased latency.

Rehman et al., 2026 presented the Blockchain-Enabled Secure and Anonymous Data Sharing (BS-ADS) model for secure exchange of information within the Cloud Integrated IoT (CIoT) world by using Aggregate Key Searchable Encryption (AKSE) coupled with blockchain technology to achieve confidentiality, integrity, anonymity, and efficient revocation. The use of the decentralized and immutable characteristics of blockchain allows for both transparent and privacy-compliant data sharing.

Roehrs et al., 2021 introduced an Omni-PHR—Multi Blockchain for Personal Health Records (PHRs) to help solve interoperability and distribution issues with how existing health care blockchains are currently designed and implemented. The authors created a prototype to test their architecture and evaluate how well it met these goals. The results of their experiments showed that the Omni-PHR architecture provides support for processing PHRs across distributed environments comparable to traditional systems.

Cernian et al., 2020 developed PatientDataChain, a system for storing PHRs from a variety of different sources, including IoT sensors and Clinical health systems and providing a single view of the entire healthcare value chain. The PatientDataChain prototype was validated with a proof of concept from a medical clinic in Bucharest that used data from 100 Patient Data Chain patients and processed 1000 transactions.

George et al., 2022 developed MediTrans, the patient-centric data access management system that uses blockchain technology to securely share patient-managed PHR information with hospital EHR systems. The system uses the combination of CP-ABE (Ciphertext-Policy Attribute-Based Encryption) and blockchain technology to allow for fine-grained and time-limited access control to patient data. The system was built using the Ethereum blockchain and integrated with OpenEMR, and results from testing the MediTrans prototype demonstrated that it provided viable performance in terms of the size of data being processed and user load when using a secure blockchain-based PHR management system.

- Thwin and Vasupongayya 2019 suggested a blockchain-based personal health record (PHR) model that is built for better privacy, tamper-resistance, and flexibility in access control. This model is composed of a framework containing proxy re-encryption and multiple advanced cryptographic methods to provide fine-grained authorizing, consent revocation, and auditing features. Security analysis shows that the model is robust against breaches of privacy, and the results of performance evaluation show that the performance of the proposed solution is improved over previously available blockchain-based PHR solutions, making it a firm candidate for secure healthcare data.
- Bisht et al., 2023 introduced a a dynamic and efficient PHR-sharing framework integrating Searchable Symmetric Encryption (SSE), blockchain technology, and the InterPlanetary File System (IPFS). Their model implemented a multi-faceted solution that guarantees data confidentiality, allows for the formulation of verifiable search results, provides forward security, and eliminates centralization via decentralized storage, thorough formal proofs help to establish a secure model's resilience through experiential study to empirically demonstrate that a secure framework for sharing PHR exists within decentralised environments.
- Murthy et al., 2024 developed a permissioned blockchain-based system supporting (Hyperledger Fabric) to support secure PHR/PHI sharing between health care providers; their model used an IPFS off-chain data storage solution with a Byzantine Fault Tolerance (BFT) consensus algorithm to protect patient privacy through smart contracts that allowed for fine-grained control of patients over their respective PHRs/PHIs. Performance benchmarks were developed using Hyperledger Caliper, and it was confirmed that the proposed model had low latency, low CPU usage, and low memory consumption while providing a foundation for secure telemedicine applications.
- Lv et al., 2025 developed an MedExChain a cross-chain data-sharing system—that allows users to exchange secure PHR data using multiple blockchain networks (for example IoMT networks). MedExChain uses a Cryptographic Reverse Firewall (CRF) in conjunction with blockchain auditing mechanisms to provide security against threats originating from inside and outside of a network. The security of MedExChain was validated through the use of BAN

logic, Scyther tool, CPA and ASA analyses which proved its security robustness and performance evaluation suggests the system can operate effectively on devices with limited computational and communication capabilities.

- Abdellatif et al., 2020 proposed ssHealth, which provides the foundation for a healthcare architecture based on the use of the blockchain and edge computing to detect, monitor and respond to epidemics. The ssHealth system supports safe medical data transfer between Distributed Health Care Entities and provides flexibility in terms of configuring Quality of Service (QoS) requirements. The flexible architecture of ssHealth enhances the interoperability (the ability to intercommunicate) and security of exchanging health-related data across both national and international health care systems.
- Wang et al., 2025 proposed a Dynamic Grouping-based Practical Byzantine Fault Tolerance (DG-PBFT) consensus algorithm for improving adaptability/reliability within blockchain healthcare environments. This algorithm dynamically reorganizes nodes/participants while implementing a reputation-based weighted federated averaging method to evaluate participant performance. Through its contribution towards improved consensus efficiency and trust management within a distributed medical data environment, the framework lays the groundwork for future applications of blockchain technology in the healthcare industry.
- Liang et al., 2024 developed the Medical Consortium Blockchain-Dynamic Security Configuration (MC-DSC). The MC-DSC adjusts the amount of blockchain resources according to the degree of urgency related to healthcare information. Identity management and encryption add an extra security layer to this system while increasing its performance. Performance statistics reveal performance improvements offered by MC-DSC over standard blockchain applications for healthcare.
- Khan et al., 2022 developed BIoMT, an architecture of consortium blockchain built using the Hyperledger Fabric platform for securely exchanging data on the Internet of Medical Things (IoMT). In this architecture, the proxy re-encryption method is used for ensuring privacy, whereas smart contracts facilitate the registration of devices and maintenance of ledgers. Therefore, in terms of transparency and efficiency, it offers a highly improved architecture compared to decentralized healthcare systems.
- Chanumolu & Nagamani (2025) suggested a hybrid Smart Healthcare Model utilising machine learning techniques along with blockchain technology by combining predictive models (disease risk assessment) as well as time series analysis to monitor health-related progressions. Block chain technology allows permanent storage and limits access to all parties responsible for accessing information; using homomorphic encryption and differential privacy methods offers additional protection of patient confidentiality during data analysis.
- Sunitha and Kumar 2025 introduced a multi-layered security framework which merges attribute-based access control (ABAC) with the Ethereum blockchain that provides cloud-based healthcare organisations overall security. The proposed architecture consists of hybrid encryption, secret sharing techniques for key management; smart contracts to automate the enforcement of policies and multiparty computation for preserving individual privacy. Table 3 shows comparative analysis of blockchain-based approaches for cloud-based PHR systems.

**Table.3 Blockchain Approaches for Cloud PHR: A Comparison**

| Research Work | Study Context (Parameters) | Designed Solution | Identified Research Gaps |
|---|---|---|---|
| Dong et al. (2023) | Patient-controlled PHR sharing, consent management, Hyperledger Fabric | Blockchain-enabled Access Control (BAC) model for secure, consent-driven PHR sharing | Scalability concerns and dependency on specific blockchain framework |
| Costa et al. (2022) | Interoperable PHR management, workload & network scalability evaluation | Permissioned distributed ledger architecture using Hyperledger Fabric | High latency for write operations; blockchain performance lower than traditional databases |
| Rehman et al. (2026) | Secure CIoT data exchange, confidentiality, anonymity, revocation | BS-ADS model integrating AKSE with blockchain | Complexity of integrating searchable encryption with blockchain at scale |
| Roehrs et al. (2021) | Geographically distributed PHR interoperability | OmniPHR multi-Blockchain architecture | Limited real-world deployment validation and |

| | | | |
|---|---|---|---|
| | | | interoperability standardization |
| Cernian et al. (2020) | Integration of heterogeneous PHR sources (IoT + clinical systems) | PatientDataChain decentralized PHR platform | Limited scalability validation beyond proof-of-concept |
| George et al. (2022) | Patient-centric access control, EHR–PHR interoperability | MediTrans using Ethereum + CP-ABE | Ethereum-based systems may face gas cost and scalability issues |
| Thwin & Vasupongayya (2019) | Privacy, tamper resistance, consent revocation | Blockchain model with proxy re-encryption | Computational overhead of cryptographic operations |
| Bisht et al. (2023) | Decentralized storage, verifiable search, forward security | SSE + Blockchain + IPFS-based PHR sharing | Storage and indexing efficiency in large-scale deployments |
| Murthy et al. (2024) | Secure PHR sharing, telemedicine, off-chain storage | Hyperledger Fabric + IPFS + BFT consensus + smart contracts | Off-chain storage security management complexity |
| Lv et al. (2025) | Cross-chain PHR exchange, IoMT environments | MedExChain with CRF and blockchain auditing | Cross-chain synchronization and interoperability challenges |
| Abdellatif et al. (2020) | Epidemic monitoring, edge computing, QoS adaptability | ssHealth blockchain-edge healthcare framework | High architectural complexity and deployment cost |
| Wang et al. (2025) | Consensus optimization, trust management | DG-PBFT with reputation-based federated averaging | Requires further validation in heterogeneous healthcare networks |
| Liang et al. (2024) | Dynamic blockchain resource allocation based on data urgency | MC-DSC adaptive configuration model | Limited discussion on interoperability with other chains |
| Khan et al. (2022) | IoMT secure communication, device automation | BIoMT consortium blockchain with proxy re-encryption | Resource constraints in large IoMT deployments |
| Chanumolu et al. (2025) | ML-based disease prediction + blockchain security | Hybrid ML + Ethereum + homomorphic encryption | Integration complexity and computational overhead |
| Sunitha & Kumar (2025) | Multi-layered cloud healthcare security | ABAC + Ethereum + hybrid encryption + MPC | High implementation complexity in real-world healthcare systems |

**3.3 Data Privacy**

- Zhang et al., 2018 have designed an effective attribute-based data sharing that is sensitive to the privacy and that supports offline encryption and key generation. The delicate assigned values specified in a framework for accessibility are not communicated utilizing a ciphertext in the proposed system. By conducting the majority of encryption activities without depleting the battery, the offline/online encryption technique lessens the computational overhead on mobile users. In mobile cloud computing, the offline process ensures that the system is appropriate for resource-constrained data proprietors and that the attribute authority can offer effective registration services.
- Zhang and Lin 2018 have developed an e-health system diagnosis advancement through a BSPP (blockchain-based secure and privacy-preserving PHI sharing) program. First, the data formats and collaboration methods regarding the two distinct types of blockchains — consortium and private—are developed. The private blockchain is where the PHI is kept., and the consortium blockchain is in charge of keeping track of the PHI's secure indexes. It is suggested to use

public key encryption together with keyword searching for the PHI sharing protocol. The physician is permitted to examine and access the desired past medical history to aid in diagnosis after obtaining trapdoors from the patient.

- Liu et al 2018 suggested a BPDS (privacy-preserving data sharing) for EMR based on blockchain. With BPDS, the created EMRs are safely maintained within the clouds, and the reserved metrics are stored in an impenetrable blockchain consortium. Patients can fully control their EMRs by using the suggested BPDS, and Corporations or individuals may readily acquire the records without worrying about the privacy of the patients.
- Lu et al., 2019 have implemented a distributed multiple-party, privacy-preserving data-sharing structure for industrial IoT applications. First created a distributed multiple-party secure data sharing architecture driven by blockchain. Then, using privacy-preserving federated learning, they transformed the data exchanging challenge into an ML problem. Offering the data sources rather than the real data contributes to maintaining confidentiality. Last but not least, they integrated a joined understanding of the consensus mechanism of the permissioned blockchain so that the computational labor necessary for agreement may arise applied to federated instruction as well.
- Gupta et al., 2019 presented a layered architecture based on sensitivity that is effective at protecting data privacy and security in cloud environments. Depending on the layered security process, the suggested method minimizes the overall overhead of the cloud service. To achieve advanced stability between utility and information security, encryption, watermarking algorithms, and hashing, and are creatively and uniquely mixed at each layer. This method included a feature to identify the defective node causing leakage of highly confidential data at the most vulnerable levels. Finally, experimental analysis is done to evaluate how well the layer-based technique performs.
- Fan et al., 2018 introduced a blockchain-based plan to address privacy worries in 5G mobile networks. In our method, the difficulty of managing keys is also much reduced. To guard the user's data security, we utilize a mix of encryption technology and access control policies. The cloud's encrypted data storage can only be retrieved by those who can comply with the access strategy. Additionally, users can create granular access policies to achieve better data control. This approach increases the user's freedom in regulating information; for instance, it can limit both who can access the data and how long it can take.
- Raghavendra et al., 2025 introduced a secure encryption framework to facilitate proxy-based search and access to cloud-based Personal Health Records (PHRs) for remote patient monitoring. Patient medical data is encrypted prior to being uploaded to the cloud to support confidentiality of the information. Access to the data management platform is limited to authorized hospitals or research organizations, while physicians who are authorized will have limited access to the PHR data for the treatment of their patients.
- Anandhi et al., 2026 developed a new authentication protocol for cloud-based healthcare systems utilizing Improved Elliptic Curve Cryptography (Im-ECC). The protocol uses the Adaptive Secretary Bird Optimization (AdSB) algorithm for optimal key generation, increasing security and decreasing the computational overhead associated with the use of keys. The protocol consists of three main phases: registration, login and authentication; all for ensuring secure access and sharing PHR data in the cloud.
- Verma et al., 2024 developed a blockchain based cloud security system that incorporates a modified Blowfish encryption algorithm with an optimal key generation procedure based on Elephant Herding Optimization with Opposition-Based Learning (EHO-OBL). The system increases the integrity of medical records and enhances the ability to authenticate people who access the system. In comparative evaluations of other encryption methods, the proposed method generated better keys than traditional methods, demonstrating improved data protection and increased efficiency when storing healthcare records in the cloud.
- Karthikeyan et al., 2025 presented a Symmetric Fine-Tuned Blowfish (SFB) encryption solution for electronic health records stored in hybrid cloud environments. The authors used adaptive key configurations and an emphasis on encrypting data with a private key before uploading to cloud storage as part of the implementation in order to achieve enhanced protection for cloud data.
- Praveen et al., 2023 conducted research into the security challenges associated with outsourcing health care data to cloud computing providers and developed a rule-based information sharing policy through the use of a Data Capture and Auto Identification Reference (DACAR) framework. A Single Point of Contact (SPC) for cloud-hosted buckets of data enables scalable, secure, and cost-effective storage, and the new method improves data integrity, confidentiality, and query performance while supporting secure, large-scale health care deployments. Figure 4, shows how cloud data privacy is maintained.

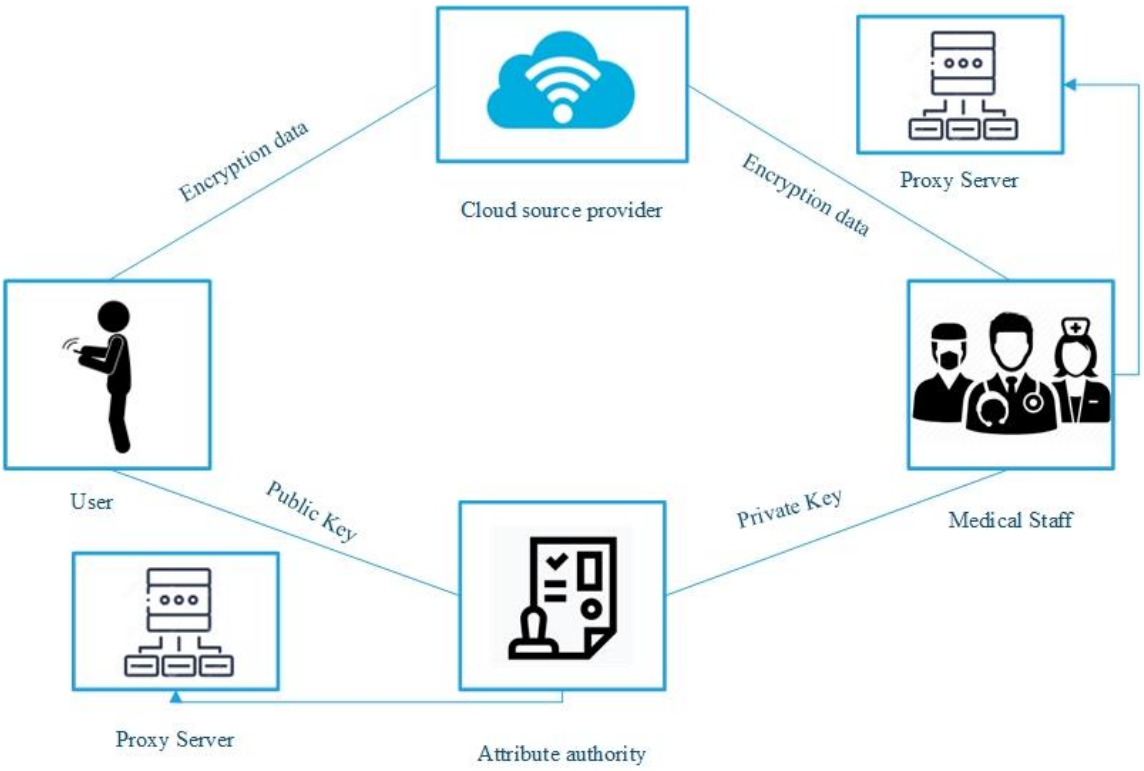


**Figure.4 Data Privacy in Cloud Service Provider**

### 3.4 AI-Integrated Security Models

Security models integrating Artificial Intelligence (AI) are currently being used in cloud-based PHRs and EHRs to improve threat identification, access control, data privacy protection, and compliance with regulatory policies. While conventional security frameworks rely on predetermined rules, security models that utilize AI allow intelligent threat detection and prediction, as well as access monitoring. The latest developments in such security models include the use of machine learning algorithms, including CNNs, LSTMs, and other ensemble classifiers, which allow for predicting possible data breaches or attacks in healthcare clouds.

Nagarajan and Geetha 2023 presented an AI-powered privacy-preserving healthcare security system framework using federated learning and differential privacy to conduct decentralized learning without divulging patients' data. The proposed framework features governance components to validate compliance, orchestrate policies, and facilitate end-to-end communication in line with global healthcare legislation. The experimental evaluation results show improved resistance to cyberattacks, reduced susceptibility to attacks, and greater operational continuity within the collaborative healthcare environment.

Al-Otaibi et al., 2025 aimed to enhance the current status, for that, they designed an Intrusion Detection System (IDS) using Artificial Intelligence (AI) technology with CNN and Lightweight Authentication Protocols tailored specifically for Medical Sensor Network (MSN). The CNN system, tested using the NSL-KDD database, achieved high IDS detection performance according to proven IDS evaluation criteria. The authentication protocols ensured secure real-time communication with minimal processing overhead, thus making it appropriate for the RCMD context.

Thawbaan et al., 2025 explored cybersecurity vulnerabilities in healthcare facilities despite the implementation of frameworks like NIST, GDPR, and HIPAA. Their model an integrated security approach built on three levels: a mathematical model (A-VIAM) of quantifiable vulnerabilities; threat detection using AI-based Machine Learning techniques; and a customized Healthcare Security Governance Framework. The integration of content analysis and quantitative modeling provides a planning guide to assist organizations with reducing risk associated with cyber-attacks, thereby enhancing digital resiliency capabilities in healthcare systems.

Serra et al., 2024 suggested a new cloud-native healthcare analytics framework that supports secure AI and has the ability to process large amounts of data and allows for API interoperability. The proposed framework incorporates encrypted data exchange, zero trust, role-based access control, secure API gateways, and compliance-centric governance models within its design. The use of automated MLOps pipelines provides a means for deploying machine learning models as a

containerized microservice and enables the ongoing management of machine learning models throughout their entire lifecycle.

Kumar and Prince 2025 developed a cyber-resilient healthcare architecture that leverages federated learning, Model-Chaining Protocols (MCPs), Zero-Knowledge Proofs (ZKPs), and blockchain-based governance mechanisms. The recommended architecture will improve the security, privacy, and reliability of the data stored in the healthcare systems while incorporating an automated compliance validation system. Although the implementation process is complex, this paper outlines the guidelines on how to use artificial intelligence, blockchain, and cloud computing technologies in building a secure healthcare environment.

Kumar et al., 2022 developed a framework for the security of cloud-based personal health records (PHRs) that was designed using optimized rule-based fuzzy inference systems (ORFIS) for identifying the criticality levels of patients. The classification of patients into various criticality levels helps in securing the more important patients first. Access control policies based on graphs and anonymous authentication were used in the private cloud environment. Experimental evaluation demonstrated improved accuracy in patient criticality detection along with enhanced data access granularity and retrieval efficiency.

**3.5 Session key and Cloud Storage Security Mechanisms**

- Qikun et al., 2019 implemented an essential agreement within the group technique built on attribute authentication and privacy protection. This method for unsymmetrical group key agreement prioritizes attribute authentication and privacy protection, according to the scheme. The procedure uses technologies for identity identification based on attributes. To attain the goal of attribute-based hidden identity authentication, which prevents the leak of personally identifiable information and protects individual attribute information from revelation, the attribute is concealed via polynomial computation throughout the attribute authentication process.
- Sowjanya et al., 2019 developed a lightweight ABE key policy based on elliptic curve cryptography not using bilinear pairing and including a key update/refresh capability. The authority distributes the keys and includes direct characteristics or user withdrawal in the process. The plan is protected by elliptic curve decision-making. The results demonstrate that the suggested design is significantly more efficient in terms of the key refresh mechanism than the present competitive schemes when the operation of the proposed model is tested using an example of the AAL system. A future study is intended on ABE's multiauthority and nonmonotonic structural properties to improve the pairing-free KPABE's performance.
- Shanmuga Priya et al., 2019 implemented an improved strategy for the current model for data security. The creation of OTP via HMAC (Hash-based Message Authentication Code) is part of the suggested data security concept. For better model implementation, this article also compares the SHA and MD5 algorithms. This study utilized certain encryption techniques to convert the source text into a format that a third party cannot understand. The last key concern is data availability; it is regarded as a hazard related to the cloud computing environment. The authors have defined overarching design standards for a cloud environment, which result from the need to manage pertinent risks and vulnerabilities. 27 Therefore, as a strong authentication method for this circumstance, we have suggested using active single-time passwords utilizing dual authentication, which employs mobile as an authentication device.
- Wang et al., 2020 discussed an innovative IoT-based three-factor authentication system via chaotic maps for cloud computing. The session key safeguard is ensured and the cost of calculation is simultaneously decreased with the aid of Chebyshev chaotic maps. The informal study demonstrates that our method can survive known assaults and accomplish desirable properties like resistance and user anonymity to the session key exposure attacks of all kinds. The semantic confidence of the session key is confirmed by the formal analysis. The suggested scheme has great security, making it particularly suitable for cloud applications that require security, including cloud-based healthcare systems.
- Martínez Pelaez et al., 2019 have implemented a new version that takes into account the steps of key negotiation, mutual authentication, and log-in to improve security. This work also provided "Evidence of connection attempt" is one section, that demonstrates the user and server's engagement. The novel method enhances earlier works by meeting security criteria and resisting well-known threats. The performance study shows that this system can satisfy security needs without a lot of processing power or communications.
- Sajay et al., 2019 have proposed a hybrid algorithm to boost cloud security using an encryption algorithm. Utilizing encryption techniques is primarily done to safeguard or preserve vast amounts of information on the cloud. To advance cloud security, this analysis merges the two types of encryptions blowfish and homographic. Security paradigms

including accessibility, data recovery, confidentiality, authentication, and data integrity are used in the cloud. It comprises cloud computing services, deployment models, security issues, and roadblocks. Using encryption methods over cloud architecture, this hybrid approach also provides a security method and greater storage.

- Ogiela et al., 2020 have presented some techniques for secret data management and Protection. Data services are a specific kind of information that needs to be secured, and this duty will be carried out through data-sharing protocols. There will be various levels of data protection, and within each level, data management and protection responsibilities will be carried out. The authors' approach to data security involves using cryptographic threshold practices to divide the confidentiality among a predetermined group of secret directors. A novel class of practices known as intelligent linguistic threshold structure is created as a result of this approach, which is simultaneously enhanced by the use of linguistic techniques for conveying the shared secret. One tool used to safeguard data in the cloud is the CAPTCHA, or Completely Automated Public Turing Test to Tell Computers and Humans Apart. It is technique of intelligent data management and protection.
- Shahzadi et al., 2020 have implemented an adaptive neural control fuzzy Inference system (ANFIS) to minimize risks and obstacles to security by using protection methods. Following the current scenario, ANFIS detected the input parameters, fuzzified the information, and merged them into the knowledge-based rule foundation. To train the data, various membership functions were applied. Process circulation is necessary to effectively manage security in cloud applications. This work examined the problem of cloud security point by point and evaluated the situation from the perspective of cloud formation.
- Wu et al., 2019 developed a cloud security model using game theory. This model can evaluate the internal safety risks in the current systems and determine if a CSP (Cloud Service Provider) or a TSP (Third-party Service Provider) would treat user data honestly. The cloud system has theoretical interior protection if a Nash equilibrium analysis of consumers and service suppliers playing a game concludes that any provider by a user would choose not to rob the information corresponding to his utility function. Users will receive more security from a semi-reliable TSP if they have at least equal levels of trust in it as they have in the CSP.
- Ganapathy 2019 implemented a cloud database that uses a CRT (Chinese Remainder Theorem)-which depends on a data conservation system to securely keep user data. The cloud database encrypted data is accessed through CRT, which is also used to create a new group key management system. The suggested CRT-guaranteed storage system uses two encryption plans containing both new encryption techniques for the first and second encryptions and unique decryption procedures. Additionally, a new formula is added to the group key creation procedure for accessing the cloud database's encrypted data on a server in the cloud. The security models' level of performance has been assessed by looking at the outcomes of the experiment.
- Zhang et al., 2019 developed a CPVPA a certificate-less public verification system, and a tardy auditor. Each audit verification performed by CPVPA is linked to a transaction on the on-chain currencies' blockchain. Additionally, CPVPA is not affected by the certificate management issue. Comparing CPVPA to other schemes, the security study shows that it offers the strongest security assurance. Additionally, we carried out a thorough performance analysis, which displays that CPVPA has consistent communication overhead and low calculation overhead. The upcoming work will be based on how to develop CPVPA on other blockchain systems. Figure 5 shows the security in the cloud storage.

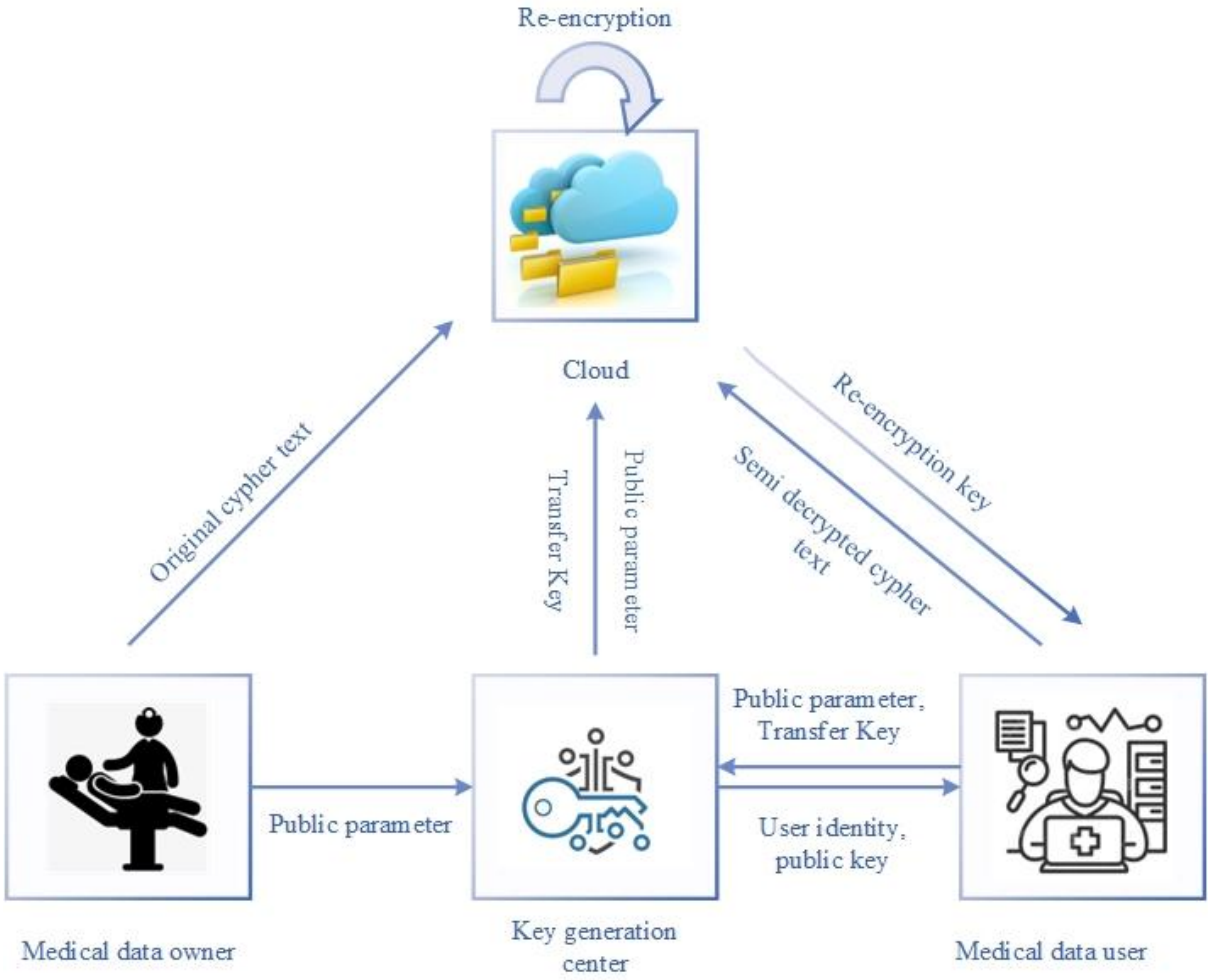


**Figure.5 Security In The Cloud Storage**

## 4. RESULT AND DISCUSSION

This section analyzes and compares the effectiveness of cryptography-based, blockchain-enabled, AI-integrated, and session key–based security mechanisms for cloud-based Personal Health Record (PHR) and Electronic Health Record (EHR) systems.

### 4.1. Comparative Security Performance

The comparative analysis presented in Table 4 provides a structured comparison highlighting the performance characteristics, advantages, and constraints of various security mechanisms used in cloud-based healthcare environments. The evaluation was conducted based on technique used, security level, access control model, scalability, key management complexity, computational overhead, and real-world validation.

**Table.4 Cloud Healthcare Security: A Comparative Analysis**

| Ref | Technique Used | Security Level | Access Control Type | Scalability | Key Management Complexity | Computational Overhead | Real-World Validation |
|---|---|---|---|---|---|---|---|
| (43) | Attribute-Based Encryption (Offline/Online) | High | Attribute-Based | High | Moderate | Low (mobile-optimized) | Experimental analysis |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| (44) | Blockchain-based PHI sharing (BSPP) + PKE | High | Blockchain + Keyword Search | High | High | Moderate | Prototype evaluation |
| (45) | Blockchain-based BPDS for EMR | High | Patient-centric control | High | Moderate | Moderate | Performance testing |
| (46) | Blockchain + Federated Learning | Very High | Permissioned blockchain | High | High | Moderate | Industrial IoT simulation |
| (47) | Layered Encryption + Watermarking + Hashing | High | Layer-based sensitivity | Moderate | Moderate | Moderate | Experimental validation |
| (48) | Blockchain + Encryption + Policy Control | High | Policy-based granular control | High | Moderate | Moderate | 5G scenario testing |
| (49) | Proxy-based Encrypted PHR Search | High | Restricted institutional access | Moderate | Moderate | Low | Security analysis |
| (50) | Im-ECC + AdSB Optimization | High | Authentication-based | High | Low–Moderate | Low | Simulation results |
| (51) | Blockchain + Optimized Blowfish (EHO-OBL) | Very High | Authentication-based | High | Moderate | Low–Moderate | Comparative evaluation |
| (52) | Symmetric Fine-Tuned Blowfish (SFB) | High | Private-key controlled | Moderate | Low | Low | Hybrid cloud testing |
| (53) | Rule-based DACAR Framework | Moderate–High | Rule-based policy | High | Moderate | Low | Deployment study |
| (60) | Attribute-based Group Key Agreement | High | Attribute Authentication | High | High | Moderate | Formal security proof |
| (61) | ECC-based KP-ABE (Pairing-free) | High | Key-policy ABE | High | Moderate | Low | AAL system testing |
| (62) | HMAC-based OTP + Dual Authentication | Moderate–High | Two-factor authentication | High | Low | Low | Comparative hash testing |
| (63) | Chaotic Map-based 3FA | Very High | Three-factor authentication | High | Moderate | Low | Formal & informal analysis |
| (64) | Mutual Authentication + Key Negotiation | High | Session-based | High | Moderate | Low | Performance evaluation |
| (65) | Hybrid Blowfish + | High | Encryption-based | Moderate | Moderate | Moderate | Experimental results |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Homomorphic Encryption | | | | | | |
| (66) | Threshold Cryptography + Linguistic Secret Sharing | Very High | Multi-level threshold | High | High | Moderate | Conceptual & applied study |
| (67) | ANFIS-based Risk Detection | Moderate –High | Adaptive fuzzy control | High | Low | Moderate | Simulation study |
| (68) | Game-Theoretic Cloud Model | Moderate | Trust-based model | High | Low | Low | Theoretical validation |
| (69) | CRT-based Encrypted Cloud Database | High | Group key management | Moderate | High | Moderate | Experimental evaluation |
| (70) | CPVPA Blockchain Auditing | Very High | Certificate-less Public Audit | High | Moderate | Low | Performance analysis |

Publisher-based analysis of the 70 reviewed papers reveals that a substantial portion of the research is published by renowned international scientific publishing houses, which together publish around 49 percent of the total number of papers. It clearly suggests the high-tech and engineering-based nature of cloud computing healthcare security research, especially in topics like blockchain-based architecture, cryptography-based techniques, federated learning, and artificial intelligence-based intruder detection. Table 5 shows the distribution of the 70 reviewed research papers based on their publishers.

**Table.5 Publisher-Wise Distribution Of Reviewed Research Articles**

| Publisher | Approx. Count |
|---|---|
| Springer | 18 |
| IEEE | 16 |
| Elsevier | 9 |
| MDPI | 8 |
| Nature Group (Scientific Reports / NPJ) | 2 |
| Taylor & Francis | 2 |
| Wiley | 2 |
| Other Journals / Regional Publishers | 13 |
| Total | 70 |

### 4.2. Challenges in Securing Cloud-Based PHR Systems

Despite considerable progress in cryptography, blockchain technology, and artificial intelligence-powered security measures, certain issues still exist in cloud-based Personal Health Records (PHR) systems:

#### 4.2.1 Complex Key Management

Attribute Based Encryption (ABE) and multi-authority models are complicated when it comes to key generation, distribution, revocation, and updating. There is still difficulty in handling the dynamic access of users and the situation of emergency access.

#### 4.2.2 High Computational Overhead

The complexity of advanced encryption mechanisms, homomorphic encryption, and blockchain consensus protocols leads to higher costs of encryption and decryption, which is not appropriate for IoT healthcare devices due to their limited resources.

#### 4.2.3 Scalability Issues
With the increasing number of users, health care providers, and IoT devices, sustaining the performance of the system along with latency and secure exchange of information becomes difficult, especially with the use of blockchain technology.

#### 4.2.4 Communication Overhead
High authentication, key exchange, and synchronization overhead result in network congestion and increased delays, which impact real-time healthcare applications.

#### 4.2.5 Storage Overhead
Encrypted data, metadata, access policies, and blockchain ledger replication significantly increase storage requirements.

#### 4.2.6 Emergency Access Control
Accessing patient information safely but instantly during emergencies while maintaining their confidentiality is still a problem yet to be solved.

#### 4.2.7 Interoperability and Standardization
Various health care platforms and cloud vendors adopt heterogeneous standards, hindering seamless and secure transfer of data.

#### 4.2.8 Regulatory and Compliance Issues
Meeting regulatory requirements for healthcare (HIPAA and GDPR equivalent laws) in various legal systems is complicated.

#### 4.2.9 Insider and Advanced Persistent Threats
Despite the best encryption efforts, insider attacks and advanced cyberattacks still present dangers to confidential medical information.

#### 4.2.10 Integration of AI Security Models
Intrusion detection systems using AI need high-quality data sets and may be subject to adversarial attacks as well as model poisoning.

## 5. CONCLUSION
In this study, the literature on security solutions for cloud-based PHR has been thoroughly reviewed from the period of 2016 to 2026, including cryptographic-based approaches, blockchain-based schemes, authentication and session keys, artificial intelligence-assisted security models, and hybrid approaches. The results indicate that attribute-based encryption and blockchain technology have been extensively used to provide confidentiality, integrity, and fine-grained access control, whereas the latest research tends to incorporate artificial intelligence and federated learning into PHR security solutions. While significant advancements have been made, the following obstacles still need to be addressed: high computation cost, scalability problems, key management difficulties, interoperability problems, and lack of wide implementation. The results, in general, show that there is no one solution that solves all the security problems. Hence, it can be seen that the hybrid system, which integrates cryptographic techniques, blockchain technology, and AI technologies, will be the best way forward.

**DECLARATIONS:**

**FUNDING**

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

**CONFLICTS OF INTEREST**

The authors declare that we have no conflict of interest.

**COMPETING INTERESTS**

The authors declare that we have no competing interest.

**DATA AVAILABILITY STATEMENT**

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real world data with appropriate permissions.

**AUTHOR'S CONTRIBUTIONS**

Author 1: Naveen John J
He participated in the methodology, Conceptualization, Data collection and writing the study
Author 2: I. Shatheesh Sam
He Performed the Analysis the overall concept, writing and editing

**REFERENCES**

[1] Khan, F.A., Rahman, A., Alharbi, M. and Qawqzeh, Y.K., 2020. Awareness and willingness to use PHR: a roadmap towards cloud-dew architecture based PHR framework. Multimedia Tools and Applications, 79(13), pp.8399-8413.

[2] Kusunose, M. and Muto, K., 2023. Public attitudes toward cloud computing and willingness to share personal health records (PHRs) and genome data for health care research in Japan. Human Genome Variation, 10(1), p.11.

[3] Lee, S.Y., 2020. Cloud based Blockchain Technology for Personal Health. International Journal of Advanced Nursing Education and Research, 5(3), pp.47-54.

[4] Hosseini, A., Emami, H., Sadat, Y. and Paydar, S., 2023. Integrated personal health record (PHR) security: requirements and mechanisms. BMC Medical Informatics and Decision Making, 23(1), p.116.

[5] Kuppuswamy, P., Sundaram, S. and John, R., 2020. Designing Framework of Cloud Health Record (CHR) System for Patient Health Information Storage: A New Prophecy. International Journal of Computer & Software Engineering, 5(1).

[6] Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and security of cloud computing: a complete guideline. Symmetry, 15(11), 1981.

[7] Rodrigues, Bruno, Ivone Amorim, Ivan Silva, and Alexandra Mendes. "Patient-centric health data sovereignty: an approach using Proxy re-encryption." In European Symposium on Research in Computer Security, pp. 199-215. Cham: Springer Nature Switzerland, 2023.

[8] Das, Sangjukta, and Suyel Namasudra. "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure." IEEE Transactions on Industrial Informatics 19, no. 1 (2022): 821-829.

[9] Saravanan, N., & Umamakeswari, A. (2021). HAP-CP-ABE based encryption technique with hashed access policy based authentication scheme for privacy preserving of PHR. Microprocessors and Microsystems, 80, 103540.

[10] Chen, Biwen, Tao Xiang, Debiao He, Hongwei Li, and Kim-Kwang Raymond Choo. "BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records." IEEE Transactions on Information Forensics and Security 18 (2023): 3171-3184.

[11] Exceline, C. Eben, and Jasmine Norman. "Biometric based Multi-Authority Inner Product Encryption for Electronic Health Record." EAI Endorsed Transactions on Pervasive Health and Technology 5, no. 20 (2022): e1.

[12] Dong, Yibin, Seong K. Mun, and Yue Wang. "A blockchain-enabled sharing platform for personal health records." Heliyon 9, no. 7 (2023).

[13] Costa, Thiago Bulhões da Silva, Lucas Shinoda, Ramon Alfredo Moreno, Jose E. Krieger, and Marco Gutierrez. "Blockchain-based architecture design for personal health record: development and usability study." Journal of Medical Internet Research 24, no. 4 (2022): e35013.

[14] Roehrs, Alex, Cristiano A. da Costa, Rodrigo R. Righi, André H. Mayer, Valter F. da Silva, José R. Goldim, and Douglas C. Schmidt. "Integrating multiple blockchains to support distributed personal health records." Health Informatics Journal 27, no. 2 (2021): 14604582211007546.

[15] Cernian, Alexandra, Bogdan Tiganoaia, Ioan Sacala, Adrian Pavel, and Alin Iftemi. "PatientDataChain: a blockchain-based approach to integrate personal health records." Sensors 20, no. 22 (2020): 6538.

[16] George, Merlin, and Anu Mary Chacko. "MediTrans—Patient-centric interoperability through blockchain." International Journal of Network Management 32, no. 3 (2022): e2187.

[17] Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-based access control model to preserve privacy for personal health record systems. Security and Communication Networks, 2019(1), 8315614.

[18] Bisht, Abhishek, Ashok Kumar Das, Dusit Niyato, and Youngho Park. "Efficient personal-health-records sharing in internet of medical things using searchable symmetric encryption, blockchain, and IPFS." IEEE Open Journal of the Communications Society 4 (2023): 2225-2244.

[19] Abdellatif, Alaa Awad, Abeer Z. Al-Marridi, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, and Ahmed Refaey. "ssHealth: toward secure, blockchain-enabled healthcare systems." IEEE Network 34, no. 4 (2020): 312-319.

[20] Khan, Abdullah Ayub, Asif Ali Wagan, Asif Ali Laghari, Abdul Rehman Gilal, Izzatdin Abdul Aziz, and Bandeh Ali Talpur. "BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts." IEEE Access 10 (2022): 78887-78898.

[21] Zhang, Yinghui, Axin Wu, and Dong Zheng. "Efficient and privacy-aware attribute-based data sharing in mobile cloud computing." Journal of Ambient Intelligence and Humanized Computing 9, no. 4 (2018): 1039-1048.

[22] Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." Journal of medical systems 42, no. 8 (2018): 1-18.

[23] Liu, Jingwei, Xiaolu Li, Lin Ye, Hongli Zhang, Xiaojiang Du, and Mohsen Guizani. "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records." In 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2018.

[24] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT." IEEE Transactions on Industrial Informatics 16, no. 6 (2019): 4177-4186.

[25] Gupta, Ishu, Niharika Singh, and Ashutosh Kumar Singh. "Layer-based privacy and security architecture for cloud data sharing." Journal of Communications Software and Systems 15, no. 2 (2019): 173-185.

[26] Fan, Kai, Yanhui Ren, Yue Wang, Hui Li, and Yingtang Yang. "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G." IET communications 12, no. 5 (2018): 527-532.

[27] Praveen, S. Phani, Balamuralikrishna Thati, Ch Anuradha, S. Sindhura, Mohammed Altaee, and M. Abdul Jalil. "A novel approach for enhance fusion based healthcare system in cloud computing." Journal of Intelligent Systems and Internet of Things 9, no. 1 (2023): 84-96.

[28] Nagarajan, Geetha. "AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes." International Journal of Engineering & Extended Technologies Research (IJEETR) 5, no. 2 (2023): 6292-6297.

[29] Kumar, Sarvesh, Mohammed Abdul Wajeed, Rajashekhar Kunabeva, Nripendra Dwivedi, Prateek Singhal, Sajjad Shaukat Jamal, and Reynah Akwafo. "Novel method for safeguarding personal health record in cloud connection using deep learning models." Computational intelligence and neuroscience 2022, no. 1 (2022): 3564436.

[30] Qikun, Zhang, Li Yongjiao, Gan Yong, Zheng Chuanyang, Luo Xiangyang, and Zheng Jun. "Group key agreement protocol based on privacy protection and attribute authentication." IEEE Access 7 (2019): 87085-87096.

[31] Sowjanya, K., Mou Dasgupta, Sangram Ray, and Mohammad S. Obaidat. "An efficient elliptic curve cryptography-based without pairing KPABE for Internet of Things." IEEE Systems Journal 14, no. 2 (2019): 2154-2163.

[32] ShanmugaPriya, S., A. Valarmathi, and D. Yuvaraj. "The personal authentication service and security enhancement for optimal strong password." Concurrency and Computation: Practice and Experience 31, no. 14 (2019): e5009.

[33] Wang, Feifei, Guosheng Xu, Guoai Xu, Yuejie Wang, and Junhao Peng. "A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure." Wireless Communications and Mobile Computing 2020 (2020).

[34] Martínez-Peláez, Rafael, Homero Toral-Cruz, Jorge R. Parra-Michel, Vicente García, Luis J. Mena, Vanessa G. Félix, and Alberto Ochoa-Brust. "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances." Sensors 19, no. 9 (2019): 2098.

[35] Sajay, K. R., Suvanam Sasidhar Babu, and Yellepeddi Vijayalakshmi. "Enhancing the security of cloud data using hybrid encryption algorithm." Journal of Ambient Intelligence and Humanized Computing (2019): 1-10.

[36] Ogiela, Lidia, Marek R. Ogiela, and Hoon Ko. "Intelligent data management and security in cloud computing." Sensors 20, no. 12 (2020): 3458.

[37] Shahzadi, Shumaila, Bushra Khaliq, Muhammad Rizwan, and Fahad Ahmad. "Security of cloud computing using adaptive neural fuzzy inference system." Security and Communication Networks 2020 (2020).

[38] Wu, Yuzhao, Yongqiang Lyu, and Yuanchun Shi. "Cloud storage security assessment through equilibrium analysis." Tsinghua Science and Technology 24, no. 6 (2019): 738-749.

[39] Ganapathy, Sannasi. "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications." Computer Networks 151 (2019): 181-190.

[40] Zhang, Yuan, Chunxiang Xu, Xiaodong Lin, and Xuemin Shen. "Blockchain-based public integrity verification for cloud storage against procrastinating auditors." IEEE Transactions on Cloud Computing 9, no. 3 (2019): 923-937.