University of Baghdad
College of Engineering
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.joe.uobaghdad.edu.iq

Volume 29 Number 1 January 2023

State-of-the-Art in Data Integrity and Privacy-Preserving in Cloud Computing

Mariam Duraid Abdul-Jabbar *
MSc Student
University of Baghdad
College of Science
Iraq-Baghdad
mariam.doraid1201a@sc.uobaghdad.edu.iq

Yousra Abdul alsahib s.aldeen
Assist. Prof. Dr.
University of Baghdad
College of Science for women
Iraq / Baghdad
yousraalkaalesi@gmail.com

ABSTRACT

Cloud computing (CC) is a fast-growing technology that offers computers, networking, and storage services that can be accessed and used over the internet. Cloud services save users money because they are pay-per-use, and they save time because they are on-demand and elastic, a unique aspect of cloud computing. However, several security issues must be addressed before users store data in the cloud. Because the user will have no direct control over the data that has been outsourced to the cloud, particularly personal and sensitive data (health, finance, military, etc.), and will not know where the data is stored, the user must ensure that the cloud stores and maintains the outsourced data appropriately. The study's primary goals are to make the cloud and data security challenges more understandable, to briefly explain the techniques used to achieve privacy and data integrity, to compare various recent studies in both pre-quantum and post-quantum, and to focus on current gaps in solving privacy and data integrity issues.

Keywords: Cloud Computing (CC), data integrity, privacy-preserving.

احدث الطرق لتكامل البيانات والحفاظ على الخصوصية في الحوسبة السحابية

مريم دريد عبدالجبار
طالبة ماجستير
جامعة بغداد/ كلية العلوم

يسرى عبدالصاحب سيف الدين
استاذ مساعد دكتور
جامعة بغداد/ كلية العلوم للبنات

الخلاصة

الحوسبة السحابية (CC) هي تقنية سريعة النمو,التي توفر أجهزة كمبيوتر وشبكات وتخزين كخدمات يمكن الوصول إليها واستخدامها عبر الإنترنت. توفر الخدمات السحابية أموالاً للمستخدمين لانها تعمل بشكل الدفع لكل استخدام ، كما أنها توفر الوقت لأنها مرنة حسب الطلب ، وهو جانب فريد من جوانب الحوسبة السحابية. ومع ذلك ، يجب معالجة العديد من مشكلات الأمان

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2023.01.03

Article received: 28/6/2022
Article accepted: 5/8/2022
Article published: 1/1/2023

قبل أن يقوم المستخدمون بتخزين البيانات في السحابة. نظرًا لأن المستخدم لن يتحكم بشكل مباشر في البيانات التي تم الاستعانة بمصادر خارجية لها في السحابة ، وخاصة البيانات الشخصية والحساسة (الصحة ، والتمويل ، والجيش ، وما إلى ذلك) ، ولن يعرف المستخدم مكان تخزين البيانات ، يجب على المستخدم التأكد من ذلك تقوم السحابة بتخزين البيانات الخارجية والاحتفاظ بها بشكل مناسب. تتمثل الأهداف الرئيسية لهذه الدراسة في جعل تحديات الحوسبة السحابية وأمان البيانات أكثر قابلية للفهم ، وشرح بإيجاز التقنيات المستخدمة لتحقيق الخصوصية وتكامل البيانات ، ومقارنة الدراسات الحديثة المختلفة في كل من ما قبل الكم وبعده ، والتركيز على الفجوات الحالية في حل مشكلات الخصوصية وتكامل البيانات.

الكلمات الرئيسية: الحوسبة السحابية, تكامل البيانات, الحفاظ على الخصوصية

1. INTRODUCTION

The United States National Institute of Standards and Technologies (NIST) defines cloud computing (CC) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Five basic qualities, three service models, and four deployment types make up this cloud model" **(Mell and Grance, 2011)**. Cloud users can access, transfer, retrieve, and manage data in the cloud from anywhere, at any time, because of CC's massive hardware/software computer resources (elasticity) (internetwork-based repository).

Furthermore, by leveraging cloud-based services, network providers may manage large volumes of data, possibly millions of data, in seconds, delivering the same effective system services as the "supercomputers cloud" **(Shao et al., 2018).** Cloud technology is innovative even if the underlying technology is an evolutionary process since employees and users may start relatively small and become huge at a constrained speed only in accordance with their demands **(Abdulredah and Kadhim, 2020)**.

Microsoft Azure, IBM Blue Cloud, and Amazon's EC2 are the most popular cloud computing services, although there are more. Other third-party Cloud Computing providers provide data storage, computation management, and internet services. CC is flexible (on-demand), allowing service providers to migrate their data to the cloud platform progressively. It is also cost-effective because it is pay-per-use. The use of cloud computing to hold personal and sensitive data by governmental and non-governmental organizations is rapidly increasing **(Yousra and Mazleena, 2018).** Since CC's importance and popularity are growing, and it's gaining more attention from the scientific and industrial communities, many security issues, such as threats and vulnerabilities, are causing concern among users and businesses worldwide because they have no idea where their data is stored. Inside threats, account hijacking, malware injection, insufficient access control, DoS, and other data security vulnerabilities in CC are examples.

There are numerous other threats to the cloud, not only from outsiders but also from insiders who may exploit cloud security flaws to target others. These hazards could jeopardize data security, availability, and integrity **(Hiremath and Kunte, 2017)**. As a result, improved privacy preservation and data integrity techniques/methods are required to secure sensitive information/data sharing, storing, and managing data in the cloud to protect users' sensitive and personal data. To address these security concerns and issues, multiple research works concentrated on CC security, primarily privacy and integrity, and produced various methods, approaches, and strategies.

This survey aims to identify the most pressing data security issues, briefly describe the strategies and methods used to ensure privacy and data integrity, compare numerous recent research, and highlight the present gaps.

The remainder of this questionnaire is organized as follows: section 2 describes the architecture and characteristics of cloud computing, and section 3 discusses the challenges and issues of data security in cloud computing, as well as CC's privacy-preserving and data integrity solutions. In section 4, there will be a comparison of various privacy-preserving, and data, and in section 5, there will be a comparison of various privacy-preserving, and data. In section 6, the research gaps will be examined, and in section 7, the conclusion will be presented.

2. CLOUD COMPUTING OVERVIEW

2.1 CC's Architecture

Fig. 1 represents the architecture of cloud computing, and as shown in the figure, any user from anywhere can use any cloud model and any service using the internet connection.

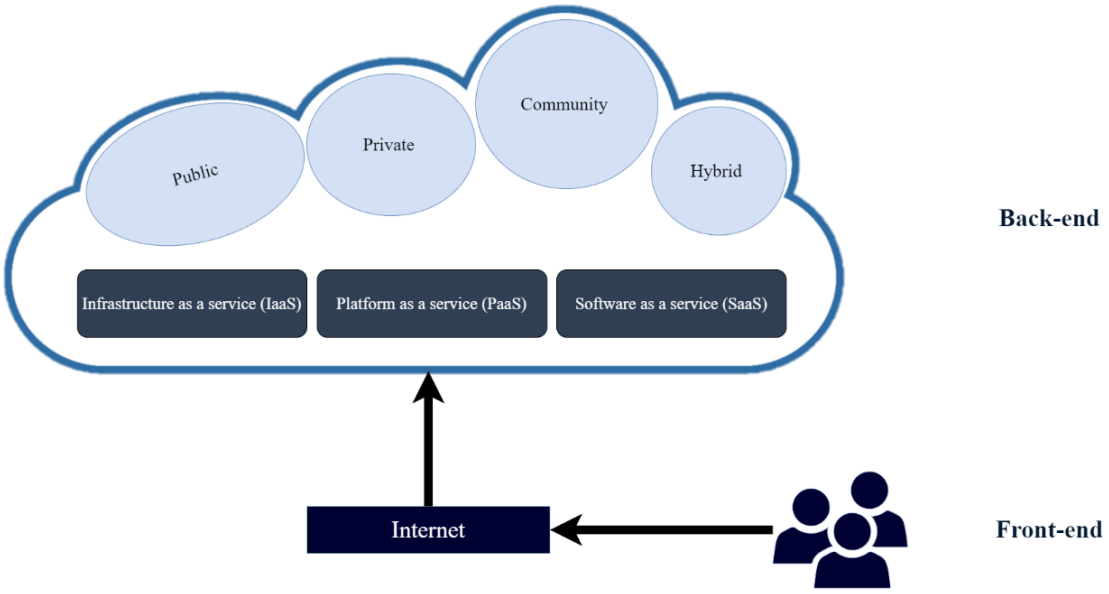

Figure 1 Cloud computing architecture

2.2 Essential Characteristics of CC by (Mell and Grance, 2011)

1- Self-service on-demand: Users can request CUP time, storage, network connectivity, server time, internet applications, and a variety of other cloud resources and have them automatically allocated without the need for human contact **(Rashid and Chaturvedi, 2019).**

2- Broad network access: is defined as the use of computing resources that are accessible through the internet or a network and can be accessed in a controlled and standard manner to improve the usage of heterogeneous systems that can be thin or fat. Popular

platforms include smartphones, tablets, laptops, and desktop computers **(Diaby and Rad, 2017).**

3- Pooling of resources: The cloud contains both physical and virtual computing resources. These resources aren't location-dependent in the sense that the user is either unaware of or unable to alter their location **(Rashid and Chaturvedi, 2019).**
4- Rapid elasticity: Tools and features can be quickly adjusted and implemented with little actual hardware contact **(Mohammed and Zeebaree, 2021).**
5- Measuring capacity: To automatically manage and optimize resource use at an abstract level relating to the sort of service they provide (e.g., bandwidth, storage, processing, and active user accounts). The use of resources can be tracked, managed, and reported, giving both the service provider and the consumer more transparency **(Mell and Grance, 2011)**

2.3 CC's Models by NIST (Mell and Grance, 2011)

Deployment Models:

1- Public cloud: Anyone who wishes to use the cloud infrastructure can do so in the public cloud. A firm, institution, government agency, or a combination of these organizations, may own, maintain, and control it. It can exist on the cloud provider's premises **(Simmon, 2018)**.
2- Private cloud: A private cloud is tailored to a certain company or industry, such as a cloud for a specific industry **(Rashid and Chaturvedi, 2019).**
3- Community cloud: Infrastructure and services are provided to organizations with the same objectives in a community cloud **(Rashid and Chaturvedi, 2019).**
4- Hybrid cloud: The cloud's resources are basically made up of two or more cloud models (public, communal, or private) that run independently and are linked by standard or customized technologies that offer data and application flexibility (e.g., cloud bursting for load balancing) **(Simmon, 2018)**.

Service Models:

1. Software as a Service (SaaS): The software can be accessed via a thin client interface, such as an internet browser (e.g., web-based email), or a program interface, via a variety of client devices. With the possible exception of restricted user-specific application configuration options, the client does not monitor or control the underlying cloud infrastructure, such as networking, servers, system software, storage, or even particular application features **(Simmon, 2018)**.
2. PaaS (Platform as a Service): It is a framework or platform that allows developers to create and deploy applications and programs over the internet without having to set up or maintain a development environment **(Mohammed and Zeebaree, 2021).**
3. IaaS (Infrastructure as a Service): The user is given the ability to allocate CPU, memory, internet, and other basic computing resources, allowing them to create and run any type of software, including applications and operating systems. Even though the users do not have management or control of the cloud infrastructure, it does have control over the operating system, memory, and application programs, as well as maybe partial control over some network elements (e.g., host firewalls) **(Mell and Grance, 2011).**

3. CHALLENGES and ISSUES of PRIVACY-PRESERVING and INTEGRITY in CLOUD COMPUTING

With the rapid technology development and the increase of its usage in most life fields, traditional computing became insufficient, so cloud computing became essential since the user doesn't work where the data is and got less control in cloud computing in addition to transition risks and sometimes a malware inside the cloud. Privacy-preserving and Data integrity have become major necessities to protect the user's data and sanative/personal information primarily in healthcare, the military, banks, etc.

3.1 Privacy

The representational features of sensitive data and the data itself are examples of sensitive information its owner does not want to be released. In general, sensitive information such as a person's income, health data, a company's financial information, and so on is referred to as "privacy" **(Fang et al., 2017).**

- Unauthorized data access
- Release of sensitive information
- eavesdropping
- Malicious cloud users or providers can reveal sensitive Data.

3.2 Data integrity: It is the process by which data owners verify the integrity and authentication of data that has been outsourced to ensure that neither unauthorized users nor devices have caused unnoticed changes to the data. For example, malicious users or systems may delete or illegally modify outsourced data. Data integrity ensures the correctness and consistency of users' data; in other words, It blocks unauthorized users and systems from altering data without being noticed **(Zhang et al., 2018).**

- Unauthorized data modification
- Loss/deletion of data
- Data corruption by cloud malware
- Tempering/replacing the data

4. PRIVACY-PRESERVING and DATA INTEGRITY TECHNIQUES in CLOUD COMPUTING

- Data splitting is a method of distributing data to several hosts at once when they are unable to interact separately. As a result, if a user wants his or her data back, he or she must access all the resource allocators to get the original data **(Mondal et al., 2020)**. Several data splitting methods are proposed to preserve Privacy. **(Zhang et al., 2013)** proposed MapReduce**.**

  Adv. faster than encryption because data is stored in several clouds and replication is required. Security is also a top consideration because the attacker will have a lower chance of gaining access to multiple clouds at once **(Mondal et al., 2020).**

  Dis. Losing the data in one cloud may make the other useless.
- Adding noise: To ensure secrecy, change confidential attributes by adding noise. Noise-adding works by multiplying or adding a randomized or stochastic number to secret numeric parameters **(Mivule, 2013).**

  Adv. Preserve the privacy, the data will not be useful even if the intruder gets access gets the data.

Dis. Adding noise corrupts data correctness.

- Tokenization is used mostly in the banking industry to replace the values on an ID card with other values that decrease an adversary's utility. This method employs unidirectional encryption techniques across an indexed function of randomly generated integers that are not mathematically derived from the original data **(El Ouazzani and El Bakkai, 2020).**
  Adv. It is now the strongest and yet most secure technique of providing authentication to access and control sensitive data.
  Dis. Complexity, expensive, risk of losing the token
- Synthetic data: This technique involves creating mathematical modeling that leverages the actual data to produce synthetic data **(Kanwal et al., 2021).** This technique uses machine learning algorithms.
  Adv. Although not revealing accurate data, the published data reserve unique characteristics **(Kanwal et al., 2021).**
  Dis. These techniques do not guarantee data integrity at the record level **(Kanwal et al., 2021).**
- Generalization: The first family of non-cryptographic anonymization approaches is a generalization, which involves modifying the scale or order of size of charterers' attributes to make them more ubiquitous **(El Ouazzani and El Bakkai, 2020).** Must popular generalization techniques l-diversity and t-closeness.
  Adv. prevents attribute disclosure, a wider range of critical attributes inside the grouping, and pruning is faster than k-anonymity **(Rajendran et al., 2017).**
- *Dis.* Although generalization can prevent singling out, it is not always effective. In reality, to avoid linkability and inference attacks, generalization necessitates using particular and advanced quantitative approaches **(El Ouazzani and El Bakkai, 2020).**
- Anonymization: is the process of completely removing any information that may be used to identify a person. It is difficult to identify people from a data collection once it has been anonymized. Organizations typically utilize this marketing and research strategy without reachingut to individuals **(Ribeiro and Nakamuru, 2019).** Popular method: k-anonymity
  Adv. protects against the disclosure of identity-less costs **(Rajendran et al., 2017).**
  Dis. Attacks: Homogeneity, Background knowledge, unsorted matching, and complementary release **(Rajendran et al., 2017),** it's not useful in all data types, e.g., images.
- Pseudonymisation (data masking): GDPR (General Data Protection Regulation) defined this technique as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. Such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" **(GDRP, 2019)**. The sensitive information/data are hidden by using an alternative fake value.
  Adv. Privacy-preserving since it helps to reduce the data's linkability to the real identity,
  Dis. Using consistent pseudonym make using a linkage attack to re-identify data easier. A recipient may attempt to reverse the pseudonyms or to re-identify based on identifying information **(Garfinkle, 2015).**

- Encryption: Data is encrypted when stored in a format that can't be read without an encryption key. For the intruder, the information is completely worthless. It is a method of converting data into ciphertext. To read encrypted information, the encryption key, sometimes known as a secret key or password is needed **(Sharma et al., 2014).** Asymmetric encryption and symmetric encryption are the two main types of encryption. Symmetric encryption encrypts and decrypts data using a secret key. However, users must first select a consensus key before implementing symmetric encryption, which is problematic for multi-user file sharing. Asymmetric encryption, often referred to as public-key encryption, is more efficient in comparison. A pair of keys are used in public-key encryption. The public key is used for encrypting data and may be delivered to others, while the private key is used for decrypting the encrypted message **(Yang et al., 2020).** The most widely used algorithms currently include the RSA, AES, ECC, SHA series, El-Gamal, MD5, and others **(Yousif and Fadahl, 2021).**
  Adv. Users with authorization can decipher the file using the associated private key, then edit or delete the ciphertext **(Yang et al., 2020).** Effectively preserves the data's privacy and protects it from being tampered with**.**
  Dis. The main limitation of encryption is key management, especially in symmetric (private key). In addition, encryption is an expensive technique.
- Trusted Third Party (TTP): is a third-party entity that enables secured interaction between the two parties that both trust it. In an Information System, a TTP aims to provide end-to-end security services that are extensible, standards-based, and applicable over domains, different geographic locations, and specialist fields **(Issis and Lekkas, 2012).**
  Adv. Manage the access and authentication like key generation and exchanging to provide better privacy and data integrity.
  Dis. The high cost performs the operation and stores the data on one central cloud/server, the risk of an intruder accessing it and losing the data if the server is down.
- Auditing: this is a process for determining the efficacy of services hosted in a cloud environment in terms of performance. Third parties typically conduct audits in order to obtain data related to various operational performances of cloud-based applications and services. The primary objectives of auditing are to i) define the data architecture, ii) manage IT risk, iii) strategically design an IT strategy, iv) manage communication, and v) implement security controls **(Kumar and Shantala, 2020).**
  Adv. Verify the integrity of the data to ensure that it is accurate and consistent.
  Dis. High cost and the need for an expert in auditing.
- Access control: The data owner (DO), a central authority (CA), a data user (DU), and a cloud server (CS) are the four entities in the centralized access control scheme. The central authority is a trustworthy center that controls access policies, distributes keys for the data user and owner, and is responsible for the centralized idea. The data owner uploads the necessary resources and data to the cloud server, which then maintains the information and provides a transmission service between the data user and the data owner. Finally, the data is received and downloaded by the data used by the access policies **(Almutairi et al., 2021)**.
  Adv. Preserve privacy and data integrity by adding policies to the data, only authorized gain access, and only performing permitted operations on the data.

Dis. There is no perfect way to use this technique. In most cases, it needs cauterized TTP, which is costly. Furthermore, it causes much overhead.

- Blockchain: is a transparent, shared, and decentralized ledger that makes recording and tracking resources easier without relying on a centralized authority. It allows two parties to interact and share resources in a peer-to-peer network in which the consensus, instead of a single centralized authority, makes decisions **(Salman et al., 2018)**.
- *Adv.* Blockchain technology has a decentralized nature, decentralized decisions, peer-to-peer systems, cryptography security, and non-repudiation assurances **(Salman et al., 2018)**.
- A hybrid method combines two or more privacy-preserving or/and data integrity techniques to get more privacy and data integrity or solve an issue in a technique by adding another.

5. COMPARISON with PREVIOUS WORKS

Various methods have been used to protect privacy and ensure data integrity in cloud computing. Some methods only protect privacy, while others only provide data integrity; many methods used only one technique to achieve these two important features, but most methods used a combination of two or more techniques and/or technologies to achieve better performance. Furthermore, some techniques include properties like as search ability. In this section, a number of well-known works in this subject will be compared, including the method they employed, what they archived, their restrictions and benefits in **Table 1**, and their features in **Table 2.**

Table 1 Summary of previous works

No.	Ref.	Method	Environment	Techniques used	Advantages and Results	Limitations
1	**(Singla, S., & Singh, J., 2012)**	Authentication and Encryption Technique	Cloud Computing	EAP-CHAP, encryption, Rijndael algorithm	Only the authorized user has access to the data. Even when an intruder has access to the data, whether by mistake or on purpose, "he or she will not be able to decrypt it."	Risk of symmetric key transmission
2	**(Hiremath, S., & Kunte, S., 2017)**	A Novel Data Auditing Approach	Cloud Computing	• AES 128-bit encryption • (SHA-256 bit) • TPA to audit	• The time taken by the System is constant to audit the files of different file sizes. • The TPA took -time to audit the files ranging between (100KB-1000KB).	Risk of symmetric key transmission
3	**(Subha, T., & Jayashri, S., 2017)**	Efficient Privacy-Preserving Integrity Checking Model	Cloud computing	digital signature (trusted third party auditor (TTPA)) Merkle Hash Tree(MHT) CA (Certificate Authority)	When there are active adversaries in the system Provides user privacy at a rate of over 95% and is capable of detecting changes in stored data.	Assuming that the (TTPA) is a trusted one, it is difficult to find a trusted TPA
4	**(Spyra, G., Buchanan, W. J., & Ekonomou, E. 2017 ,)**	Sticky policies approach	Cloud Computing	IRM, XACML Sticky Policy, IBE Sticky Policy,	Developing an OASIS XACML-compliant product is simple.	Implement using a trusted authority, it is difficult to find trusted authority
5	**(Hu, C., Li, W., Cheng, X., Yu, J., Wang, S., & Bie, R. , 2017)**	A Secure and Verifiable Access Control Scheme	Cloud Computing	Access Policy NTRU Cryptosystem	Allows the data owners to flexibly adjust data access control policies with the cloud server to update the relevant ciphertext- text and enable effective cloud data management.	
6	**(Shaheen, S. H., Yousaf, M., & Jalil, M. , 2017)**	Temper proof data distribution for universal verifiability and accuracy in the electoral process using blockchain	Group Oriented Communication	Blockchain Technology (BCT) NTRU cryptosystem,	Individual and universal verifiability, as well as transparency and accuracy, are provided for electoral data.	NTRU signature is not secure
7	**(Shao, B., Bian, G., Wang, Y., Su, S., & Guo, C., 2018)**	Dynamic Data Integrity Auditing Method Supporting Privacy Protection	Vehicular Cloud	bilinear pairing mapping BLS signature, third-party auditor	Reduce the time it takes to audit data integrity and update data dynamically.	Requires improvement that now communication's cost is somewhat higher than the document
8	**(Uchibeke, U. U., Schneider, K. A., Kassani, S. H., & Deters, R. , 2018)**	Blockchain access control Ecosystem	Cloud computing	Blockchain, access control (the Blockchain Role-Based Access Control Business Network (BRBAC BN or Blockchain Identity-Based Access Control Business network (BIBAC BN))	secure data sharing by ensuring data transparency and traceability	The stability of Hyperledger Fabric. Changes and updates are being made to the smart contract and fabric distributed ledger
9	**(Yousra, S. A., & Mazleena, S., 2018)**	New Heuristic Anonymization Technique	Cloud Computing	L-diversity measure, K -anonymity (a, k)-anonymity measure	Less execution time and Higher entropy and privacy than k-anonymity	Not useful in all data types

10	**(Kokoris-Kogias, E., Alp, E. C., Gasser, L., Jovanovic, P., Syta, E., & Ford, B., 2018)**	CALYPSO	Cloud computing	access-control policy Blockchain threshold cryptography	Transaction processing latency increases linearly with security (number of trustees) and is in the range of 0.2 to 8 seconds for 16 to 128 trustees, according to the benchmarks.	
11	**(Qiu, L., Sun, X., & Xu, J., 2018)**	Categorical quantum cryptography	cloud computing	Access control Quantum cryptography	• A simpler protocol for quantum certification, • The protocols are unconditional secure and implementable by the current technology.	vulnerable to the man-in-the- middle-attack
12	**(Tong, W., Jiang, B., Xu, F., Li, Q., & Zhong, S., 2019)**	Privacy-Preserving Data Integrity Verification	Mobile Edge Computing	• Two protocols: ICE-basic ICE-batch • Third Party Auditor (TPA)	The experimental results show that these protocols(ICE-basic, ICE-batch) are efficient.	Difficult to find trusted TPA
13	**(Farheen, S. N. , 2019)**	ENCRYPTION TECHNIQUE	Cloud Computing	AA (Attribute Authority) CA (Central Authority) NTRU cryptosystem	Allows the data owners to flexibly adjust data access control policies with the cloud server to update the relevant ciphertext- text and enable effective cloud data management.	
14	**(Divya, M., & Singaravel, G., 2019)**	Blockchain Technology for Privacy Protection	Cloud Computing	Intrusion Detection System(IDS), Number Theory, Cloudlets Mining, ,NTRU ,BlockChain.	The proposed schemes are validated with simulations and experiments.	
15	**(Hylock, R. H., & Zeng, X. , 2019)**	A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain):	Cloud Computing	BLOCKCHAIN Smart Contracts AES-128 AFGH	The results show severalnumber of obviously high-performing, low-bandwidth configurations, although these are not the strongest cryptography. The most powerful models suggest that the size of one's expected cumulative record affects their decision. Although the most efficient technique is eventually user-specific, AES-encrypted data using fixed keys, incremental server storage, and no further server-side encryption is the quickest and least bandwidth-intensive of the strongest configurations.	Only in dynamic mode, the server-side encryption works .Risk of symmetric key transmission
16	**(Tang, W., Ren, J., Zhang, K., Zhang, D., Zhang, Y., & Shen, X., 2019)**	Efficient and Privacy-preserving Fog-assisted Health Data Sharing Scheme	Cloud computing	Naive Bayes Classification, access control, Bilinear Maps, Shamir Secret Sharing	Encryption computation, storing, and energy usage all are cost-effective.	The Complexity of Shamir Secret Sharing
17	**(Xu, J., Wei, L., Wu, W., Wang, A., Zhang, Y., & Zhou, F., 2020)**	using lightweight streaming authenticated data structures	Cloud Computing	• Merkle Tree-based Fully Homomorphic encryption-based • Streaming Authenticated Data Structure (SADS).	Assures the privacy of users' data while having low overhead, remaining within the context of the "lightweight data integrity verification scheme."	
18	**(Huang, P., Fan, K., Yang, H., Zhang, K., Li, H., & Yang, Y. , 2020)**	A Collaborative Auditing Blockchain for Trustworthy Data Integrity	Cloud computing	Blockchain elliptic curve BLS signature algorithm-based (BLS-HVT)	• average auditing efficiency improves • mutual trust problem between data owner and Cloud Service Provider in cloud storage systems practically	The Complexity of Elliptic Curve

19	**(Sun, J., Ren, L., Wang, S., & Yao, X., 2020)**	A blockchain-based framework	Cloud computing	Blockchain Smart contract Bilinear map AES Symmetric searchable encryption	• Have the features of privacy protection, access control, and they are searchable.	Risk of symmetric key transmission The smart contract should not be trusted
20	**(Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. , 2020)**	AuthPrivacyChain	Cloud computing	Blockchain Smart Contract ACCESS CONTROL AES	Only users with access privileges can access resources, according to the experiment results. Can prevent not only external user attacks but also internal management attacks.	Risk of symmetric key transmission smart contract should not be trusted not an absolutely safe system in accountability
21	**(Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. , 2020)**	Blockchain technology for healthcare: Enhancingshared electronic health record interoperability and integrity	Cloud computing	Blockchain Access control Smart Contract Ethereum TTPA	Noticeably, enhance the integrity and interoperability of data.	Smart-contract should not be trusted, Low Scalability of ETHEREUM, Difficult to find trusted TPA
22	**(Gurupraka sh, J., & Koppu, S. , 2020)**	EC-ElGamal and Genetic Algorithm-Based Enhancement	Internet of things (IoT)	Elliptic Curve ElGamal blockchain, genetic algorithm(GA), LSB	• • Achieved a reduction of 20% in transaction processing time and a reduction of 22% in blocks validity processing time , as well as a 53% improvement in hash operation and quality and a 7% reduction in storage costs (increased the overall performance).	The complexity of the Elliptic Curve, the genetic algorithm is computationally expensive
23	**(Thwin, T. T., & Vasupongay ya, S., 2020)**	Blockchain-based Access Control Model for Personal Health Record System with Architectural Modelling and Simulation	Cloud computing	Blockchain, The AFGH algorithm Data access Digital signature	The blockchain-based PHR system can respond in 4 minutes for 60,000 daily accesses, according to the architectural model simulating. The results demonstrated that the blockchain-based PHR system can respond in an emergency within 8 minutes and has a low computing cost.	
24	**(A.Poornim a, Dr.D.Mahes wari2020 ،)**	Enhanced Ntru Public Key Crypto System Using Ear Feature Extraction	data transmission	NTRU Cryptosystem Biometrics(ear, RNA coding)	Generate the secret key by extracting users' ear features, which will make data encryption safer.	the collection of users biometric data can be used to identify the user identity
25	**(Tahir, M., Sardaraz, M., Muhammad , S., & Saud Khan, M., 2020)**	A Lightweight Authentication and Authorization Framework	Internet of Things (IoT)	Blockchain	In comparison to others, robust mutual authenticity and better access control reduces both communication and computational overhead costs.	not Resistance against man in the middle attack
26	**(Lashkami, S. R., Atani, R. E., Arabnouri, A., & Salemi, G. , 2020)**	A Blockchain-Based Framework	Cloud computing	Blockchain smart contract,	this Scheme is developed in such a way that it maximizes efficiency and also ensuring data accuracy.	Smart-contract should not be trusted
27	**(Lin, C. H. V., Huang, C. C. J., Yuan, Y. H., & Yuan, Z. S. S., 2020)**	A Fully Decentralized Infrastructure	Internet of Things (IoT)	Pre-shared key (PSK) encryption (NTRU) access-control authentication (MAM)	The result shows that • E2EE's elapsed time is notably smaller than MAM's; • E2EE has a gradually rising time for various data sizes. This proves how [E2EE allows resource-constrained devices to participate in the data subscription economy as providers while also ensuring tamper-proof data transmission to Accel.	Pre-shared key (PSK) Vulnerable to many attacks

28	**(Banupriya, S., Kottursamy, K., & Bashir, A. K., 2021)**	Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in a public blockchain	distributed systems, public storage systems, cloud storage systems	Blockchain. NTRU LB-HDKG	Quantum resistance, High speed,and high security,	NTRU signature is not secure
29	**(Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J., 2021)**	Analysis of Using Blockchain to Protect the Privacy of Drone Big Data	Drones	NTRU cryptosystem Blockchain	The results of the performance evaluation reveal that: • This method is effective at generating keys, performing encryptions, and decryptions; • The NTRU cryptosystem's homomorphic characteristic indicates that it provides high-security efficacy.	
30	**(Chen, Z., Wu, A., Li, Y., Xing, Q., & Geng, S., 2021)**	Blockchain-Enabled Public Key Encryption with Multi-Keyword Search	Cloud computing	Bilinear Pairing Blockchain Trusted Authority (TA) Smart Contract	• Less overhead and encryption time than compared schemas	Smart-contract should not be trusted, Difficult to find trusted TPA
31	**(Liu, T., Wu, J., Li, J., Li, J., & Li, Y., 2021)**	Efficient decentralized access control	Cloud computing	access control, blockchain Bilinear pairing	This scheme has a reduced computational overhead than SVPAC, PpBAC, and Timely CP-ABE by 25.37 %, 45.46 %, and 36.44 %, respectively. This scheme has a lower communication overhead than the scheme Timely CP-ABE by 17.16 % and is more secure, yet it is greater than the schemes SVPAC and PpBAC by 5.88 % and 39.05 %, respectively. This scheme's storage overhead is lower by 59.36 %, 20.25 %, and 61.88 %, respectively, than the schemes SVPAC, PpBAC, and Timely CP-ABE.	
32	**(Hemalatha, P. , 2021)**	Monitoring and Securing the Healthcare Data Harnessing IoT and Blockchain Technology	Internet of things (IoT)	Signature infrastructure (KSI), The timestamped algorithm, Merkle tree, Blockchain, a genetic algorithm	• Highly trusted, secure, transparent, and efficient. • The blockchain-based technology takes less time than the current systems.	The storage required by Timestamped algorithm the genetic algorithm is computationally expensive
33	**(Yang, Z., Chen, Y., Huang, Y., & Li, X., 2021)**	Protecting personal sensitive data security in the cloud with blockchain	Cloud Computing	access control Ethereum blockchain, AES128 MHT(Merkle Hash Tree) Smart contract SHA256	The trust-free model fulfills all standards for the protection of personal sensitive data while posing no additional security concerns. Furthermore, this model puts less pressure on the data owner in terms of computation and communication.	Risk of symmetric key transmission Smart-contract should not be trusted Low Scalability of ETHEREUM
34	**(Trabelsi, S., & Sendor, J., 2021)**	Sticky Policies for Data Control in the Cloud	Cloud Computing	Sticky Policies; Visualization	• Data Handling Preferences /Policies • Authorization • Obligation	it is difficult to find trusted TPA
35	**(Awadallah, R., & Samsudin, A., 2021)**	Blockchain in Cloud Computing	Cloud Computing	Blockchain Homomorphic Encryption SHA-256	• • It is simple to implement since it does not require any database or cloud computing system restructuring, • the systems may be integrated or adjusted to meet the demands of the users.	
36	**(Rajesh, M. , 2021)**	NTRU ALGORITHM	Cloud Computing	NTRU, (RIF)Real message index file,	Compared with RSA • RSA takes more -encryption time than NTRU. • less network usage in NTRU • Due to the simple multiplication of polynomial The decryption performance is faster in NTRU. • NTRU less Average Network Delay	
37	**(Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. , 2021)**	An Integrated Architecture Based on Blockchain	Cloud computing	HOMOMORPHIC ENCRYPTION (HE) BLOCKCHAIN TECHNOLOGY (BC) ETHEREUM BITCOIN	• • Using the HE scheme, a client can authorize a CSP to execute data processing. • No unauthorized or unnoticed modifications or deletions of client data are performed.	Low Scalability of ETHEREUM

Table 2 Previous works features

NO.	Privacy	integrity	confidentiality	Availability	audibility	verification	Authentication	Access control	Quantum - proof
1	✓	✓	✓	✓	×		✓	✓	✓
2	✓	✓	✓	✓	✓	✓	×		✓
3	✓	✓	✓		✓		✓	×	×
4	✓	✓	✓	✓	×			✓	×
5	✓	×	✓	✓	×	✓		✓	✓
6	✓	✓	✓		×	✓	×	✓	✓
7	✓	✓	✓		✓	✓	×		×
8	✓	✓	✓				✓	✓	×
9	✓	✓	✓		✓	✓	✓		×
10	✓	✓	✓	✓	✓		✓	✓	×
11	✓	✓	✓	✓	×		✓	✓	✓
12	✓	×	✓	×	×	×	×	×	×
13	✓	✓	✓	✓	✓			✓	✓
14	✓	✓	✓			×	×		✓
15	✓	✓	✓	✓	×	×	×		×
16	✓	×	✓	✓	×			✓	✓
17	✓	✓	✓		×	✓	✓		×
18	✓	✓	✓	✓	✓	✓	×		×
19	✓	✓	✓	✓	✓			✓	✓
20	✓	✓	✓	✓	×		✓	✓	✓
21		✓		✓				✓	×
22	✓	✓	✓		×	×	×	×	×
23	✓	✓	✓	✓	×	✓	✓	✓	×
24	✓	×	✓	✓	×	×	×	×	✓
25	✓	✓	✓	✓	×	✓	✓	✓	×
26	✓	✓	✓	✓	×			×	×
27	✓	✓	✓	✓	×		✓	✓	✓
28	✓	✓	✓	✓	×	✓	×	×	✓
29	✓	✓	✓	✓	×	×	×		✓
30	✓	✓	✓		×	✓	×	✓	×
31	✓	✓			×		✓	✓	×
32	✓	✓	✓	✓				✓	×
33	✓	✓	✓	✓	✓	✓		✓	✓
34	✓	✓	✓	✓	×	✓	×	✓	×
35	✓	✓	✓	✓	×	✓			×
36	✓	×	✓	✓	×	×	×	×	✓
37	✓	✓	✓		×	✓	×		×

Many methods have additional features in addition to those listed in Table 2. For example, the works proposed in NO. 6 and 9 successfully provide anonymization, while 19, 26, and 30 achieve search-ability even with encryption, and the works proposed in NO. 13, 25 provide the ability to modify data access control policies to the data owner while a cloud server effectively updates the associated outsourced ciphertext to provide efficient access control, while NO.16, When a malicious attack is identified in advance, the collaborative IDS will raise an alert and limit access, and vice versa, and NO. 6, 8, 15, and from 18 to 23, 25, 26, 28, and from 30 to 33, and 37 are decentralized due to the Blockchain system.

6. DISCUSSIONS and RESEARCH GAPS

Most of the listed strategies are effective in pre-quantum. We can see from the comparisons in **Tables 1** and **2** that using encryption, particularly the public key (asymmetric encryption), and encrypting the data before transferring it to the cloud (e.g., RSA, NTRU, etc.) is the most feasible way to maintain privacy. However, the private key is used in several unusual manners (symmetric encryption). We observe the approaches that use audition and hashing, but in recent works, it is highly usual to use the blockchain system for data integrity provisioning. In many circumstances, access control is used in conjunction with policies. It's vital to note that there are issues with access control, such as the necessity for a password. Trusting other parties, particularly in hardware/software management.

Quantum computers can break current cryptographic approaches, jeopardizing all "traditional" cryptosystems. Quantum cryptography and quantum communications have the potential to create "completely secure" networks **(Raban and Hauptman, 2018).** Since quantum computers are powerful enough to break the most common public-key encryption algorithm (RSA, Elliptic Curve), new secure algorithms are needed. In post-quantum cryptography, many algorithms have been proposed, the most effective of which is NTRU (N-th degree Truncated polynomial Ring Units), which is a lattice-based alternative to pre-quantum algorithms, but it is not resistant to man-in-the-middle attacks, so this issue needs to be addressed.

7. CONCLUSIONS

Traditional computing became impractical, so cloud computing was invented and became indispensable. However, despite all of its features and benefits, cloud computing has several disadvantages. The most significant disadvantage is that it targets user-sensitive personal data, compromising privacy and data integrity. This survey provides useful knowledge and understanding of the cloud and its architecture, characteristics, and models, as well as an explanation of the privacy and data integrity issues and challenges, as well as the techniques used to address those issues. Additionally, a comparison of various methods has been introduced in both general and method features to highlight the advantages and limitations of those methods, as well as in both pre-quantum and post-quantum scenarios. Finally, talk about the comparison's findings. This poll aims to assist cloud builders and data owners in determining the best and most appropriate solution for their data based on its level of privacy. It is concluded that cryptographic methods are the most suited and widely utilized in research for preserving privacy, and blockchain technology is the most widely employed for data integrity.

REFERENCES

Abdulredah, S. H. and Kadhim, D. J., 2020. New Approaches of Cloud Services Access using Tonido Cloud Server for Real-Time Applications, *Journal of Engineering,* 26(8), p. 83–99.

Almutairi, S., Alghanmi, N., and Monowar, M. M., 2021. Survey of Centralized and Decentralized Access Control Models in Cloud Computing, *International Journal of Advanced Computer Science,* 12(2).

Awadallah, R., and Samsudin, A., 2021. Using blockchain in cloud computing to enhance relational database security, *IEEE Access,* Volume 9, pp. 137353-137366.

Awadallah, R., Samsudin, A., Teh, J. S., and Almazrooie, M., 2021. An integrated architecture for maintaining security in cloud computing based on blockchain, *IEEE Access,* Volume 9, pp. 69513-69526.

Banupriya, S., Kottursamy, K., and Bashir, A. K., 2021. Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain, *Peer-to-Peer Networking and Applications,* 14(5), pp. 2813-2825.

Chen, Z., Wu, A., Li, Y., Xing, Q., and Geng, S., 2021. Blockchain-enabled public key encryption with multi-keyword search in cloud computing, *Security and Communication Networks.*

Diaby, T., and Rad, B. B., 2017. Computing: a review of the concepts and deployment models, *International Journal of Information Technology and Computer Science,* 9(6), pp. 50-58.

Divya, M., and Singaravel, G., 2019. Block Chain Technology for Privacy Protection for Cloudlet-based Medical Data Sharing, *Bonfring International Journal of Software Engineering and Soft Computing,* 9(2), pp. 43-46.

El Ouazzani, Z., and El Bakkali, H., 2020. A classification of non-cryptographic anonymization techniques ensuring privacy in big data, *International Journal of Communication Networks and Information Security,* 12(1), pp. 142-152.

Fang, W., Wen, X. Z., Zheng, Y., and Zhou, M., 544-560. A survey of big data security and privacy preserving, *IETE Technical Review,* 34(5), p. 2017.

Farheen, S. N., 2019. ACHIEVING PRIVACY OF BIG DATA IN MOBILE CLOUD USING ENCRYPTION TECHNIQUE.

Garfinkel, S., 2015. *De-identification of Personal Information.* s.l.:US Department of Commerce, National Institute of Standards and Technology..

GDPR, 2019. *General Data Protection Regulation. Art4. GDPR Definitions.* [Online] Available at: Available: https://gdpr-info.eu/art-4-gdpr/

Guruprakash, J., and Koppu, S., 2020. EC-ElGamal and Genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain, *IEEE Access,* Volume 8, pp. 141269-141281.

Hemalatha, P., 2021. Monitoring and securing the healthcare data harnessing IOT and blockchain technology, *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* 12(2), pp. 2554-2561.

Hiremath, S., and Kunte, S., 2017. *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT),* pp. 306-310.

Hu, C., Li, W., Cheng, X., Yu, J., Wang, S., and Bie, R. , 2017. A secure and verifiable access control scheme for big data storage in clouds, *IEEE Transactions on Big data,* 4(3), pp. 341-355.

Huang, P., Fan, K., Yang, H., Zhang, K., Li, H., and Yang, Y., 2020. A collaborative auditing blockchain for trustworthy data integrity in cloud storage system, *IEEE Access,* Volume 8, pp. 94780-94794.

Hylock, R. H., and Zeng, X., 2019. A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study, *Journal of medical Internet research,* 21(8).

Issis, D., and Lekkas, D., 2012. Addressing cloud computing security issues, *Future Generation computer systems,* 28(3), pp. 583-592.

Jabbar, R., Fetais, N., Krichen, M., and Barkaoui, K., 2020. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity, *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT),* pp. pp. 310-317.

Kanwal, T., Anjum, A., and Khan, A., 2021. Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities.,*Cluster Computing,* 24(1), pp. 293-317.

Kokoris-Kogias, E., Alp, E. C., Gasser, L., Jovanovic, P., Syta, E., and Ford, B., 2018. Calypso: Private data management for decentralized ledgers, *Cryptology ePrint Archive.*

Kumar, A., and Shantala, C. P., 2020. An extensive research survey on data integrity and deduplication towards privacy in cloud storage, *International Journal of Electrical and Computer Engineering,* 10(2).

Lashkami, S. R., Atani, R. E., Arabnouri, A., and Salemi, G., 2020. A blockchain based framework for complete secure data outsourcing with malicious behavior prevention, *28th Iranian conference on electrical engineering (ICEE),* pp. (pp. 1-7).

Lin, C. H. V., Huang, C. C. J., Yuan, Y. H., and Yuan, Z. S. S., 2020. A fully decentralized infrastructure for subscription-based IoT data trading, *2020 IEEE International Conference on Blockchain (Blockchain),* pp. 162-169.

Liu, T., Wu, J., Li, J., Li, J., and Li, Y., 2021. Efficient decentralized access control for secure data sharing in cloud computing, *Concurrency and Computation: Practice and Experience.*

Lv, Z., Qiao, L., Hossain, M. S., and Choi, B. J., 2021. Analysis of using blockchain to protect the privacy of drone big data, *IEEE,* 35(1), pp. 44-49.

Mell, P., and Grance, T., 2011. The NIST Definition of Cloud Computing, *NIST.*

Mivule K., 2013. Utilizing noise addition for data privacy, an overview. *arXiv,* p. 1309.3958.

Mohammed, C. M., and Zeebaree, S. R., 2021. Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review, *International Journal of Science and Business,* 5(2), pp. 17-30.

Mondal, A., Paul, S., Goswami, R. T., and Nath, S., 2020. Cloud computing security issues & challenges: A review, *2020 International Conference on Computer Communication and Informatics (ICCCI),* January, pp. 1-5.

Qiu, L., Sun, X., and Xu, J., 2018. Categorical quantum cryptography for access control in cloud computing, *Soft computing,* 22(19), pp. 6363-6370.

Poornima, A., and Maheswari, D., 2020. Enhanced Ntru Public Key Crypto System Using Ear Feature Extraction, *European Journal of Molecular & Clinical Medicine,* 7(11).

Raban, Y., and Hauptman, A., 2018. Foresight of cyber security threat drivers and affecting technologies, *Foresight.*

Rajendran, K., Jayabalan, M., and Rana, M. E., 2017. A study on k-anonymity, l-diversity, and t-closeness techniques, *IJCSNS,* 17(12), p. 172.

Rajesh, M., 2021. SECURE DATA TRANSMISSION IN CLOUD STROAGE SYSTEM USING NTRU ALGORITHM, *IJISER,* 8(5).

Rashid, A., and Chaturvedi, A., 2019. Cloud computing characteristics and services: a brief review, *International Journal of Computer Sciences and Engineering,* 7(2), pp. 421-426.

Ribeiro, S. L., and Nakamura, E. T., 2019. Privacy protection with pseudonymization and anonymization in a health IoT system: results from ocariot, *IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE),* pp. 904-908.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., and Samaka, M., 2018. Security services using blockchains: A state of the art survey, *IEEE Communications Surveys & Tutorials,* 21(1), pp. 858-880.

Shaheen, S. H., Yousaf, M., and Jalil, M., 2017. Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain, *2017 13th International Conference on Emerging Technologies (ICET),* pp. 1-6, IEEE.

Shao, B., Bian, G., Wang, Y., Su, S., and Guo, C., 2018. Dynamic Data Integrity Auditing Method Supporting Privacy Protection in Vehicular Cloud Environment, *IEEE Access,* Volume 6, pp. 43785-43797.

Sharma, S., Gupta, G., and Laxmi, P. R., 2014. A survey on cloud security issues and techniques. *arXiv:1403.5627.*

Simmon, E., 2018. Evaluation of cloud computing services based on NIST SP 800-145, *NIST Special Publication, 500, 322.*

Singla, S., and Singh, J., 2012. Cloud data security using authentication and encryption technique, *Global Journal of Computer Science and Technology.*

Spyra, G., Buchanan, W. J., and Ekonomou, E. 2017. Sticky policies approach within cloud computing, *Computers & Security,* Volume 70, pp. 366-375.

Subha, T., and Jayashri, S., 2017. Efficient privacy preserving integrity checking model for cloud data storage security, *2016 Eighth International Conference on Advanced Computing (ICoAC),* pp. 55-60, IEEE.

Sun, J., Ren, L., Wang, S., and Yao, X., 2020. A blockchain-based framework for electronic medical records sharing with fine-grained access control, *Plos one,* 15(10).

Tahir, M., Sardaraz, M., Muhammad, S., and Saud Khan, M., 2020. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics, *Sustainability,* 12(17).

Tang, W., Ren, J., Zhang, K., Zhang, D., Zhang, Y., and Shen, X., 2019. Efficient and privacy-preserving fog-assisted health data sharing scheme, *ACM Transactions on Intelligent Systems and Technology (TIST),* 10(6), pp. 1-23.

Thwin, T. T., and Vasupongayya, S., 2020. Performance Analysis of Blockchain-based Access Control Model for Personal Health Record System with Architectural Modelling and Simulation, *Int. J. Networked Distributed Comput,* 8(3), pp. 139-151.

Tong, W., Jiang, B., Xu, F., Li, Q., & Zhong, S., 2019. Privacy-preserving data integrity verification in mobile edge computing. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS) (,* pp. pp. 1007-1018).

Trabelsi, S., and Sendor, J., 2021. Sticky policies for data control in the cloud, *2012 Tenth Annual International Conference on Privacy, Security and Trust, IEEE,* pp. 75-80.

Uchibeke, U. U., Schneider, K. A., Kassani, S. H., and Deters, R., 2018. Blockchain access control ecosystem for big data security, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* pp. pp. 1373-1378.

Xu, J., Wei, L., Wu, W., Wang, A., Zhang, Y., and Zhou, F., 2020. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system, *Future Generation Computer System,* Volume 108, pp. 1287-1296.

Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., and Yu, K. , 2020. AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud, *IEEE Access,* Volume 8, pp. 70604-70615.

Yang, P., Xiong, N., and Ren, J., 2020. Data Security and Privacy Protection for Cloud Storage: A Survey, *IEEE Access,* Volume 8, pp. 131723-131740.

Yang, Z., Chen, Y., Huang, Y., and Li, X., 2021. Protecting personal sensitive data security in the cloud with blockchain, *Advances in Computers, Elsevier,* Volume 120, pp. 195-231.

Yousif, S. T., and Fadahl, Z. A., 2021. ProposedSecurity Framework for Mobile Data Management System, *Journal of Engineering,* 27(7), p. 13–23.

Yousra, S. A., , Mazleena, S., 2018. A new heuristic anonymization technique for privacy preserved datasets publication on cloud computing, *Journal of Physics: Conference Series,* 1003(1), p. 012030.

Zhang, J., Chen, B., Zhao, Y., Cheng, X., and Hu, F., 2018. Data security and privacy-preserving in edge computing paradigm: Survey and open issues, *IEEE Access,* Volume 6, pp. 18209-18237.

Zhang, X., Yang, L. T., Liu, C., and Chen, J., 2013. A scalable two-phase top-down specialization approach for data anonymization using MapReduce on cloud, *IEEE Transactions on Parallel and Distributed Systems,* 25(2), pp. 363-373.