IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 6, December, 2023, pp. 1467-1477
Journal homepage: http://iieta.org/journals/isi

Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions

Swetha Gadde[1*], Gutta Srinivasa Rao[1], Venkata Srinivasu Veesam[1], Madhulika Yarlagadda[2], R. S. M. Lakshmi Patibandla[3]

[1] Department of Information Technology, R.V.R & J.C College of Engineering, Guntur 522019, Andhra Pradesh, India
[2] Department of Computer Science & Engineering, Maturi Venkata Subba Rao Engineering College, Hyderabad 501510, Telangana, India
[3] Department of Computer Science & Engineering, KLEF (Deemed to be University), Vaddeswaram 522502, Andhra Pradesh, India

Corresponding Author Email: ursgadde@gmail.com

https://doi.org/10.18280/isi.280604

Received: 29 August 2023
Revised: 24 November 2023
Accepted: 4 December 2023
Available online: 23 December 2023

Keywords:
cloud computing, data sharing, two factor authentication, cryptography, cloud storage, security challenges, data privacy, access control, cloud security

ABSTRACT

Cloud computing has emerged as a pivotal trend across both commercial and academic sectors, offering substantial storage capabilities to service providers and end-users. However, the security of data within cloud environments remains a paramount concern, primarily due to insufficient access controls. This concern is addressed herein through a systematic literature review, which underscores the shared responsibility model, the ubiquitous nature of data access, and the associated breach risks. The importance of enforcing rigorous security protocols to maintain data integrity, confidentiality, and availability is emphasized, as these are vital to stakeholders relying on cloud-based services. The current work presents an analytical review of two-factor authentication (2FA) and cryptographic measures, advocating for their combined implementation to bolster the security frameworks of cloud systems. The survey meticulously examines existing research on cloud computing vulnerabilities, security mechanisms, and the underlying challenges. It is posited that ongoing enhancements and innovations in security practices are critical for countering evolving threats and safeguarding data in an increasingly digital landscape. An exhaustive evaluation of the latest advancements in cryptography is conducted, aiming to ensure secure and authenticated access control for outsourced and encrypted cloud data across diverse user groups. The findings herein serve as a foundation for researchers to refine and develop robust cloud data storage systems. The survey underscores the need for the creation of advanced encryption algorithms, authentication protocols, and intrusion detection systems. Such developments are instrumental in mitigating risks, establishing trust, and preserving the confidentiality and integrity of data stored in cloud infrastructures.

1. INTRODUCTION

The advent of advanced network technology has catalyzed a significant expansion in computing resources, enhancing data storage capabilities across numerous organizations [1]. These resources, managed by third-party entities, are accessed via the Internet and encompass a broad spectrum including storage, interfaces, hardware, network, and services [2]. The flexibility afforded by such resources enables users to harness computing power, infrastructure, and applications tailored to their specific service requirements, allowing for remote data access through various applications and information systems [3]. Traditionally, cloud computing (CC) is characterized by its agility, cost efficiency, scalability, and independence from location and device constraints [4-6].

However, the security of sensitive data stored within these systems is of paramount concern. A multitude of studies has been dedicated to investigating the myriad challenges that cloud storage presents, with a predominant focus on issues of security, regulation, privacy, and performance [7, 8]. The potential for service failure and the threat posed by malicious users also necessitate rigorous consideration from both providers and consumers. The trend toward cloud storage as a solution for managing large data volumes is tempered by concerns over data leakage, which can deter user adoption of cloud services. Consequently, security and privacy concerns have been prioritized in the context of cloud services.

A survey by Price Waterhouse Coopers (PwC) revealed that after revelations of National Security Agency (NSA) surveillance activities, 54 percent of German organizations perceived cloud computing as insecure [NSAB] [9]. In response, the implementation of robust security measures, particularly for outsourcing encrypted data and periodically verifying data integrity and availability, has become imperative. Decisions concerning security mechanisms must address challenges such as burdensome key management in the storage of encrypted data, access control, and the implications of frequent data checks on bandwidth consumption.

The evolution of cryptography in the twentieth century, largely driven by the widespread adoption of personal computers (PCs) and the expansion of networks, has witnessed the introduction of innovative cryptographic systems. The seminal work of Diffie and Hellman in 1976 introduced the world to the concept of asymmetric cryptography [5]. This was followed by the establishment of the RSA algorithm by Rivest, Shamir, and Adelman in 1978 [RSA78]. Subsequently, Shamir's prolific contributions continued to shape the field with threshold schemes, identity (ID)-based cryptographic systems, and fully homomorphic encryption. Concurrently, the independent proposals of elliptic curve cryptography by Koblitz and Miller marked a significant advance in cryptographic methodologies [10].

The landscape of cloud storage technology, wherein clients' private data are entrusted to third-party service providers, has been revolutionized by the emergence of advanced cryptographic techniques, such as quantum cryptography, to address burgeoning security concerns [11]. The responsibility of Cloud Service Providers (CSPs) extends to ensuring controlled access to the data repositories they manage. Fundamental to the viability of cloud storage systems are the dual imperatives of expansive storage capacity and low operational costs [12]. However, the migration of critical and sensitive data to cloud-based environments is contingent upon the resolution of pervasive security and privacy challenges. To confront these issues, secure cloud storage architectures, fortified by the application of efficient cryptographic techniques, have been investigated and deployed to mitigate the aforementioned risks [13, 14].

Identified Research Gap: While CSPs strive to optimize storage and processing time, enhancing system flexibility, the dual challenges of ensuring robust security and adherence to user-defined security policies are significant obstacles to thwarting unauthorized access. This paper contends with the paucity of systematic reviews dissecting the evolving and contemporary research milieu associated with data outsourcing. The intention is to forge a conduit for communication and collaboration between the academic sphere and industry stakeholders. Through the dissemination of knowledge and the cultivation of profound interest, this work aspires to proffer strategic insights that will streamline the processes of cloud adoption, migration, management, and maintenance for a diverse user base.

The principal motivation underpinning this study is the recognition that the increasing uptake of cloud computing amplifies the potential risks to data security and privacy. Innovative security measures are imperative to sustain this trend, ensuring robust data protection and nurturing trust in the progressive evolution of cloud technologies.

The crux of this paper lies in a meticulous analysis of cutting-edge security solutions for cloud storage, with a concentrated examination of two-factor authentication (2FA) mechanisms as a bulwark against data breaches. In the realm of cloud storage, cryptographic techniques are pivotal; this paper juxtaposes such techniques with alternative methods, thereby elucidating the strengths and weaknesses inherent in current practices. This survey is crafted to serve as a cornerstone for future research endeavors, fostering the development of more robust cryptographic solutions for cloud storage security.

The contributions of this review are manifold:

(1) A comprehensive understanding of cloud computing (CC) is developed, with a particular emphasis on user security and privacy. The conveyance of information across potentially unsecured cloud servers is scrutinized, alongside associated security issues and threats. A spectrum of security auditing practices is explored, revealing the critical nature of such measures for cloud security assurance.

(2) The efficacy of two-factor data protection strategies, such as Enhanced Access Control and Reduced Vulnerability to Password Attacks, is dissected to ascertain their role in safeguarding outsourced cloud data. These strategies are examined through various lenses—goals, objectives, and assessment details, including focus, depth, and scope. The integration of 2FA within security auditing is also scrutinized, offering valuable insights and future directions.

(3) An assortment of cryptographic-based approaches enabling 2FA is cataloged, emphasizing the triad of confidentiality, integrity, and authentication in the face of adversarial actions. This synthesis serves as a guidepost for researchers selecting optimal cloud data security strategies for both academic and industry applications.

(4) Detailed expositions of various review methodologies are presented, taking into account features, privacy, security, and functional requirements. Furthermore, the paper sketches out research trajectories that address the evolving demands of the dynamic cloud environment, with a nod to energy conservation, storage efficiency, processing, and availability imperatives.

By weaving together the threads of cryptography and 2FA, the paper posits that cloud storage systems can proactively confront security challenges. Such foundational security measures are critical for the implementation of nuanced cloud security techniques.

In essence, this survey endeavors to furnish a holistic analysis of the data outsourcing landscape within cloud services, pinpointing unresolved security issues. It seeks to construct a bridge linking the academic community with industry practitioners by spotlighting emergent research, underscoring the necessity of communication, collaboration, and systematic review. The organization of the paper is deliberate, delving into the intricacies of user data storage in cloud services, delineating security concerns, and advocating solutions through a structured critique of extant research and the unresolved quandaries of data outsourcing.

2. BACKGROUND INFORMATION

A foundational understanding of cloud computing (CC) is indispensable for grappling with the nuanced specifics of its operations, benefits, challenges, and the diverse array of service and deployment models. Cloud computing applications are leveraged by a plethora of vendors, including but not limited to Google, Microsoft, Amazon, and International Business Machines (IBM). It is anticipated that cloud computing will become an integral component of the operational infrastructure for myriad enterprises that prioritize data security. At the base of the cloud computing architecture lies cloud storage, which underpins the services provided to the upper layers. Its role in managing voluminous datasets and safeguarding them within the cloud ecosystem is critical [15]. The National Institute of Standards and Technology (NIST) posits that cloud computing should manifest five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These characteristics encapsulate the core principles driving the evolution and innovation of Information Technology (IT) infrastructures. Additionally, NIST has delineated a framework for cloud computing, categorizing it into four principal models: Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud [16].

The general perception of cloud storage solutions, such as Google Drive and Dropbox, is often oversimplified to that of a network disk. However, this perception belies the complexity of cloud storage, which constitutes more than just a network disk and is indeed a critical aspect of cloud computing that handles the storage and backup of substantial datasets [17]. It is through the cloud that client data are stored and safeguarded, facilitating data recovery and ensuring the security of information when access is required.

The imperative to thoroughly comprehend these foundational concepts is underscored by the aim of this survey, which is to rigorously evaluate and scrutinize the security measures employed within cloud storage systems. The focus is specifically trained on cryptographic techniques, two-factor authentication (2FA), and access control mechanisms. This survey endeavors to dissect the efficacy, associated challenges, and future directions of these security facets in fortifying data confidentiality, integrity, and user authentication within the dynamic realm of cloud computing environments.

In the landscape of cloud storage technology, a paradigm shift has been observed wherein massive, scalable, and low-power shared storage resources are facilitated through the integration of distributed, virtualized, and diverse technologies [18]. A salient advantage of secure cloud storage is the impediment it poses to unauthorized data interception; attackers are unable to compromise the integrity of the data without proper authorization from the data originator [19].

To safeguard the confidentiality of customer information, the deployment of cryptographic technology within cloud storage has been necessitated. The robustness of cryptographic schemes is predominantly contingent upon the security of the underlying cryptographic keys. Authentication protocols have been employed to authenticate both the cloud servers and the users, thereby enabling the auditing and authorization of cloud users. Cryptographic methods are predominantly applied to ensure the secure storage of data. The transmission of data in an encrypted form is rendered more secure through the application of both symmetric and asymmetric cryptographic techniques. Cloud servers proffer a suite of cryptographic tools designed to protect the privacy of outsourced data and to ensure that only authorized users are granted access to the decryption keys [20].

Security initiatives have been predominantly driven by collaborations such as the Fast IDentity Online (FIDO) alliance and Open Authentication (OATH) [21]. Implementations of FIDO Universal 2nd Factor (U2F) / FIDO2 protocols, which incorporate encryption and two-factor authentication-related physical keys, have been documented.

Lang et al. [22] utilized various frameworks—drawing on the work of Bonneau et al. [23] to evaluate the efficacy of security keys, gathering authentication data from Google services. The study revealed that the implementation of security keys facilitated efficient authentication with minimum support incidents across specific platforms. A two-phase study by Das et al. examined the usability of the Gmail Yubico security key in a controlled laboratory setting with student participants. The study found that incentives for using the Yubico security key were not significant factors in its adoption, which in turn constrains unauthorized access by cloud users. Colnago et al. [24] explored the adoption of Duo 2FA at a university, offering users one of four 2FA key options, yet observed that less than 1% opted for this security measure. Das et al. [25] identified issues with improper use of Yubico security keys that could compromise the intended level of security. Concurrently, Das et al. [25, 26] highlighted the concern of security key loss as a significant risk factor.

This background elucidates the critical elements of cryptography, Two-Factor Authentication (2FA), and access control mechanisms, which are integral to the objectives of the current survey.

3. RELATED WORK BASED ON CRYPTOGRAPHIC ALGORITHM

The work related to the proposed analysis of data security approaches is described as follows. The purpose of this overview is to provide a comprehensive understanding of existing research, highlighting the scope of methodologies, challenges, and innovative solutions explored in ensuring data confidentiality, integrity, and user authentication within cloud computing environments.

Alouffi et al. [27] reviewed cloud security threats and mitigation issues with security risks such as leakage and data tampering. The CSP was identified with security issues for cloud service deployment and implementation in a Systematic literature survey. It also identified the rarely used data of Facebook and Instagram for evaluating the proposed model. It was identified that blockchain is a partnering technology to mitigate security issues. Abdulsalam and Hedabou [28] reviewed privacy and security issues with an adaptive research solution for CC. Several literatures were reviewed with the mitigation of security threats with the analysis of different solutions.

Jebali et al. [29] analyzed emerging and current research on confidentiality and privacy concerns with interference control and potential issues in data outsourcing. Research efforts were introduced to enable user privacy in Database-as-a-Service (DaaS) technology with communicating and non-communicating servers.

Mohammad Khalid Imam Rahmani et al. [30] reviewed trust challenges with the analysis of the blockchain framework. The solution was provided in terms of security and decentralization. The review included research questions, related articles, research methods, software used, and data retrieval.

Belguith et al. [31] provided a comprehensive analysis of various attribute-based cryptographic approaches for cloud sharing services. A detailed discussion of various review schemes was provided based on security, privacy, supported features and functional requirements. Nassif et al. [32] provided SLR of cloud security and Machine Learning (ML) approaches by categorizing security threats, performance outcomes, and ML approaches.

Table 1 gives a comparison of various cryptographic methods in cloud security. Alouffi et al.'s [27-32] research shows the performance variation of different techniques.

By addressing these limitations, this survey aims to provide a consolidated, comparative, and forward-looking analysis that bridges gaps in the current literature, offering insights into integrated security strategies specifically tailored for cloud storage systems.

Table 1. Comparison of existing approaches

Reference	Year	Prevailing Framework	Elementary Concept	Security Feature	Efficiency of Cost
Alouffi et al. [27]	2021	Data intrusion, data storage in CC	Auditing, Elliptical Curve Cryptography (ECC), Intrusion detection system	data confidentiality, data integrity, and availability	Communication cost
Abdulsalam and Hedabou [28]	2022	Cloud security approaches	Privacy security threats and security flaws with an adaptive solution	Integrity, accountability, and privacy	Cost is based on the deployment procedure, which increases the overhead
Jebali et al. [29]	2021	For increasing flexibility, optimizing storage, improving data manipulation, and decreasing processing time	Database-as-a-service approaches	confidentiality	Query execution cost
Rahmani et al. [30]	2022	Secure and reliable service based on trust management	Blockchain, trust management protocol	Scalability, resource utilization	Economies of scale, resource cost
Belguith et al. [31]	2022	User control loss over cloud storage	Cryptography techniques, attribute based cryptography	Security, privacy, storage efficiency, and availability	Storage, computational, and operational cost
Nassif et al. [32]	2021	Prevent and detect attacks to mitigate security gaps against Distributed Denial-of-Service (DDoS)	ML approaches	Confidentiality, privacy	-

4. RESEARCH METHOD

The systematic literature review methodology serves as a powerful tool to consolidate existing knowledge, uncover gaps, and offer a structured and evidence-based foundation for further research, decision-making, or practical implementations in a given field. The SLR process is generally developed for medicinal research. It gives particular standards and rules to enable experts to conduct a formal and impartial survey that recognizes, evaluates and rewrites writing to answer a directing exploration question. SLR gives researchers reasonable inspiration for new work and gives complete confirmation to control basic leadership. SLR is valuable to professionals and requires a far-reaching and objective scope of sought writing. For the exploration questions, the most popular optional words/ideas and their equivalents are distinguished in order to broaden our literature coverage. In our review of secure cloud storage approaches, some crucial studies are neglected. However, there are still constraints; thus, every effort was made to employ a variety of synonyms for the important search phrases. Another limitation is related to digital libraries, which are not having any physical boundary for data access. It permits multiple users to access the same data at the same time worldwide.

A. Search Keywords

The search articles' recognizable proof is an objective of the inquiry procedure that examined the CC and systems services because of the cloud storage framework. It centers on the factor of research that influences their acknowledgement. The search procedure utilizes online logical databases for the survey. By choosing the most suitable search, words characterized a question string. The examination questions are utilized in the databases to build an inquiry string. The search keywords consist of the subsequent steps:

- Based on research questions, categorize major keywords,
- For the major keywords, identify alternative words and synonyms,
- Search string encompasses variations of the terms related to two-factor data security, cryptography, and cloud storage. Using Boolean operators (AND, OR) helps in retrieving literature that covers all specified concepts or variations of the defined terms.

Table 2. Search keywords

Line	Keywords
1.	Cloud computing
2.	Data Sharing
3.	Cryptography
4.	Security; cloud storage

Table 2 gives details about the search keywords, which is essential to know the concept of this survey. These keywords are related to cloud security.

B. Selection of Sources

The selection of sources is from journal papers and conference papers; it provides the approved outcomes and gives more knowledge about the technique. A systematic and transparent approach in the search process ensures that the literature review captures relevant publications, minimizes bias, and forms the basis for a comprehensive analysis and synthesis of existing knowledge on the chosen topic. The inquiry strings were connected to titles, theoretical and assemblage of studies; the search was directed from 2000 until 2022 using the online logical database. Most of the journals or articles are considered from this time period. In this year, most of the recent research has been published with the requirement of a dynamic cloud storage system. It is suitable to evaluate the solution for the current problem associated with cloud security. The survey is studied to take some distributed papers in both journals and conferences. Springer Digital Library, Google Scholar, Elsevier, ACM Digital Library, IEEE Xplore, and Science Direct have mostly accepted search engines for literature and databases.

5. SECURE INFORMATION SHARING OVER UNTRUSTED CLOUD STORAGE SERVICES

This section discusses secure data sharing within a cloud. For secure sharing, the data owners should develop a mechanism for secure execution in CSP for data confidentiality and integrity. The CSP has some advantages so that it can modify or control the data in the system [33, 34]:

- In a cloud storage system, the data will be stored by the data owner, which must be confidential in the cloud. In any situation, the CSP shouldn't be capable of compromising data confidentiality.
- The data owner does data sharing; the owner has full control over the data sharing. The receiver can assess the data anytime and anywhere in the cloud. Due to this, the cloud provider has no right to enter the data into the cloud.
- The correct user receives data sharing authorization; the unauthorized user cannot assess cloud storage data.

If data confidentiality is not ensured with the CSP, then the data sharing is fully controlled by the data owner. With approval given by the proprietor, the assigned client would then get information kept on the cloud. The procedure should not give any privilege to the cloud supplier for accessing the information. Data get to authorization is assigned to the expected client, as it were. Different clients, who are not the authorization holder, ought not to be able to practice the consent to get information. Figure 1 shows secure sharing on a cloud.

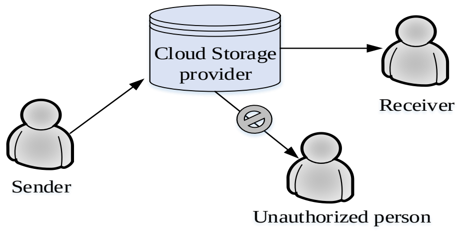

Figure 1. Secure sharing on a cloud

CC is used in many applications in academics and industries for enabling data storage, processing and management. It addresses the open issues related to the security and privacy of outsourced data. Because of dynamic scalability and observation, outsourced cloud applications have unlimited infrastructure and security boundaries. It has the nature of multi-tenancy and virtual resource sharing to support a considerable amount of users. It has sensitive information, and hence the confidence level and threats are required to be analyzed. Anonymous profile threats, including compliance, auditing, logging, hardening, and patching, make the risk of confidential information.

The integration of cryptographic methods and access control mechanisms within cloud storage systems ensures a higher level of security, addressing the vulnerabilities associated with data sharing over the cloud.

6. ORGANIZATION OF CLOUD SECURITY ISSUES IN CLOUD DATA STORAGE

One of the most critical parts of CC is data storage. Security and data storage over distributed computing was the major problem in CC. The issue is because of the fast increment of online applications and web gadgets. This section examines the security issue in cloud storage, for example, data warehouse (DWH), anonymity, accessibility, reliability service, data loss and leakage, cryptography, integrity and confidential issue, and so forth [20, 35].

A. DWH

DWHis used for reviewing the different customer teams alongside their security needs. By integrating data from various sources, several approaches are developed to provide a high computing storage system. It is utilized for guiding management decisions. A DWH is created by incorporating several database sources which support decision making, analytical reporting, Adhoc and structured queries. The decision making can be achievable from data which has been integrated, cleaned, and consolidated. It provides a multi-dimensional or generalized view for consolidated data, which requires clustering or classification [36]. It is an exceptionally tremendous gadget, and security is an essential prerequisite for usage for conveying DWH. In the Quality of Service (QoS), storage security is essential. The DWH mostly presents three fundamental issues: integrity, confidentiality, and accessibility.

B. Anonymity

Anonymity is a process or technique to obscure owner data identity based on the published information and key data preventing information. In the cloud storage system, there is an increase in anonymity because of non-suitable privacy measures. This causes a de-anonymity attack in the cloud storage system. The hidden identity of adversary threats and re-identification is some weakness problem in anonymity. Anonymous access provision approach was provided with symmetric encryption or hashing approaches. Evolving anonymous access provision improves data security by maintaining integrity and confidentiality without affecting computational complexity [37].

C. Accessibility

Providing high accessibility to the customer is the major benefit of the cloud system. It is based on the objective of making the client get information at anytime from anywhere. It provides hardware as demanded by authorized users and mainly offers software. An attack such as a DDoS or Denial of Service (DoS) attack is a network attack based on the multi-tier architecture. In a multi-tier architecture, which is helped through both running and load balancing on various servers. This approach is based on some network attacks, such as DoS or DDoS attacks**.** Due to the flooding attack, the cloud storage system lacks an availability feature. Another major issue of availability in the cloud is malicious storage data. Flexibility can be enabled with increased productivity and cooperation for accessing data from anywhere at any time. An efficient cloud storage system is developed based on the features and benefits of cloud based approaches [38].

D. Data loss and leakage

Loss of data may happen when any disaster damages the stored data, even if there is no backup. The fundamental worries of cloud clients are lost protection, trust and the direct impact of the SLA approach. In cloud usage, information leakage influences the web application in web applications also affected by data leakage. Leakage data is private in nature, and it is considered confidential. Data loss can be occurred due to system failure or deletion of some information. Several communication and control packages are evaluated and analyzed during the cloud process for data leak detection [39].

Figure 2 mentions the cloud security issues classification.

E. Cryptography

Cloud cryptography is applied to mitigate the security challenges of a CC system. But still, there are some challenges to overcoming this problem. A discrete logarithmic problem in ECC [40] and a prime factorization problem in RSA [41] is the major concern of the cloud storage system based on cryptography. Elliptic Curve Discrete Logarithm Problem (ECDLP) is used with XOR or gate function. It reduces the infrastructure cost and considers the shared resource accessibility in cloud based environment. A robust approach is provided for securing private cloud storage, which prevents unauthorized access to resources [42]. Cloud cryptography has concerns like computation efficiency, poor key management, and verifiable data.

F. Integrity and confidentiality issues

Integrity, confidentiality, and availability (CIA) are the three essential difficulties for cloud storage. Confidentiality refers to the data to the end party received with confidentiality. It is mainly required between two entities for transferring confidential messages. Data integrity describes that the information transmitted between two entities is verified for finding, deleting, and manipulating original data [43]. Integrity is the most basic data framework component to protect the data from a third party deleting or modifying information. To guarantee the integrity and confidentiality, the cloud information should follow Atomicity, Consistency, Isolation, and Durability (ACID) [44] properties. Malicious, incorrectly categorized security parameters or mistakenly arranged hypervisor and Virtual Machines emerge security issues in the cloud. Violation of respectability and classification in the cloud may happen due to the multi-inhabitant nature of the cloud.

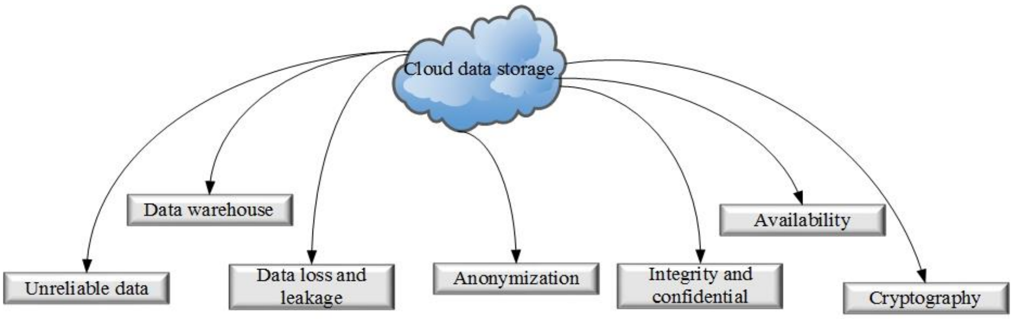

Figure 2. Classification of cloud security issue

7. OVERVIEW OF TWO FACTOR DATA SECURITY PROTECTION MECHANISM

The 2FA is significant in web security since it neutralizes the risk related to compromised passwords. In case of password guessed, hacked or phished, it restricts the intruder's access with a second factor. It contains an additional security layer for the authentication process, making it harder for the attacker to access an online account or a person's device. Even though the password is hacked, it is not sufficient to pass the authentication check. This section gives an overview of the cloud server's security protection mechanism.

The system should have the following information. The system initializes the private key generator (PKG) and security device issuer (SDI). The private key is issued for every user, and the security device issuer also has permission to issue a security device for every user. The sender creates the cipher text, and the sender sends the cipher text to the receiver. The sender only knows the receiver's identity, and the other details of the receiver are unknown to the server [11]. The sender creates cipher text and sends the cipher text to the cloud storage. Then the receiver downloads the cipher text. The receiver receives the cipher text and has a unique identity. For decryption, the cipher text can be downloaded by the receiver. The receiver also has a private key witha security device, and this security device contains some information related to the receiver. The decryption of cipher text requires a security device and a private key [12]. In normal data sharing, the sender shares the first encrypted data with the receiver and uploads the cipher text into the cloud storage. Before storing the data, it is encrypted based on symmetric key or asymmetric encryption. Asymmetric encryption generates a digital envelope for proceeding symmetric key to the authorized entities [45].

The cloud server received the cipher text and denoted it as first-level cipher text. Then, it turns the first-level cipher text into the second level ciphers text for security purposes [13]. With the private key and security device, the receiver decrypts the cipher text. Once the receiver's security device is stolen, it can inform the security device issuer. Then the SDI updates the cipher text and gives a new SDI device to the receiver. After sending the data to the receiver, the cloud server updates the cipher text with the new SDI device. The receiver decrypted the data with his new security device and private key [14].

Figure 3 shows the structure of two factor data security protection mechanism. In the original file, along with the encrypted bytes, some additional data also needs to be stored. This defines an additional vital way to form this data, so the YubiCrypt File formation [46] was generated. While privacy preserving, it is based on providing a scalable, secure and robust system.

A. YubiCrypt Files Specification

The construction of file format is an essential tool that generates the proper way to structure the data in a file, and based upon that, only reading and writing are done. Various application designers operated and edited the existing files while it was available to the public.

Proof related to the YubiCrypt concept is described below:

YubiCrypt was developed as an idea of middleware development procedure defined in the prevailing section. Recently the token for cryptography related to Universal Serial Bus (USB) was applied as the additional two-factor module. One Time Password (OTP) was created in the authentication stage, and this token is applied to the user's data to obtain access permission from the system. The scheme was combined through the ASP.NET Identity Framework, which is recently allowed to use factors with two-factor authentication such as Short Message Services (SMS) or e-mail tokens. The key for encrypted files was derived from a user passphrase. Here a stored key was either in the Key Storage Server or on a YubiKey token. So any smart phone user or mobile user can use this system by applying Near Field Communication (NFC) capabilities of the YubiKey.

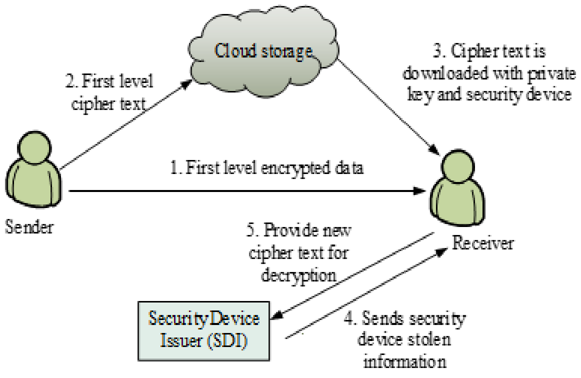
Cloud storage
2. First level cipher text
3. Cipher text is downloaded with private key and security device
1. First level encrypted data
Sender
Receiver
5. Provide new cipher text for decryption
Security Device Issuer (SDI)
4. Sends security device stolen information

Figure 3. Structure of two factor data security protection mechanism

8. CLOUD BASED VARIOUS CRYPTOGRAPHY APPROACHES SUMMARISATION

Table 3 mentions the cryptographic mechanism in the cloud. Four schemes were compared: attribute-based cryptography, PRE, content hash keying or encryption based on convergent and encryption based on homomorphic. These schemes have computational complexity related parameters. The computational complexity is moderate for proxy based approaches [47] and lower for attribute related techniques [48]. Considering encryption based on convergent complexity related to the computation depends on the number of data holders [49]. In the case of encryption based on homomorphic, precision is improved while increasing the number of users, leading to higher computational complexity [50]. When considering computational complexity, attribute based cryptography is the best one and is best for the job.

To mitigate the influence of vulnerabilities, the machine learning based approach Hidden Markov Model (HMM) is incorporated. From the HMM model, hyper alerts are transmitted to prevent the attack. K-medoid clustering is adopted for identifying the attacks by assigning soft labels for attack and data [51]. The authentication and authorization services were provided as software to enhance the security of the cloud. It was provided in an agreeable and preventive manner. In addition to the security system, the possible security threats must be analyzed to consider the security of both the authentication and authorization systems [52]. A trustworthy encryption approach based on fingerprint is provided for cloud information access. There is no uncertainty for cloud storage, and it considers cloud security while increasing the amount of data [53].

Table 3. Cryptographic mechanism in clouds

Scheme	Attribute Based Cryptography	PRE	Content Hash Keying or Encryption Based on Convergent	Encryption Based on Homomorphic
DG (Dynamic Group) Organization	Part	Entire	Entire	Entire
Use Case	Multi sharing	Single sharing	Storage	Storage
Trusted Entity	√	√	√	√
De-Duplication	x	x	√	x
Scalability	√	x	x	x
Forward Privacy	-	√	-	-
Backward Privacy	-	x	-	√
privacy	√	x	x	√

The cloud security approaches are varied based on the domain in which it is utilized. Cloud security is applicable in the area including banking, medical, and government sectors.

9. DETAILS OF SELECTED ARTICLES

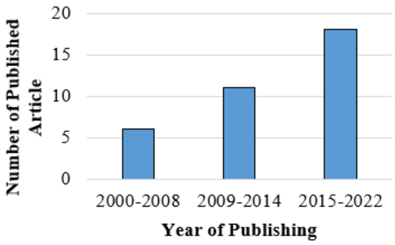

Figure 4. Number of published articles in the year 2000 to 2022

For finding essential articles, google scholar was utilized as a primary source. Using relevant CC based keywords, 35 articles are selected from ACM digital library, conference articles and other journals. The article selection based on each journal or source information is shown in Figure 4 from 2000 to 2022. The ranking was provided with a higher amount of published articles, and the year's articles published were given in Figure 4.

10. PERCENTAGE OF PUBLISHED ARTICLES

Science Direct, IEEE Xplore Digital Library, Springer Link, Web of Knowledge, ACM Digital Library and Inderscience are outstanding electronic repositories for discovering production datasets in first use. Meanwhile, nowadays, search engines are used to download the meta information. Science Direct allows collecting information on the original things from its query items. Disastrously, by applying our predefined seek string, become more than ten thousand results on this storehouse. The characterization of the articles among the four distributors appears in Figure 5. IEEE distributes 30% of the articles. Elsevier distributes 20% of the articles. Springer distributes 10% of the aggregate article in diaries, 6% of the articles in the Scientific, and the rest of the 5% in IJISS.

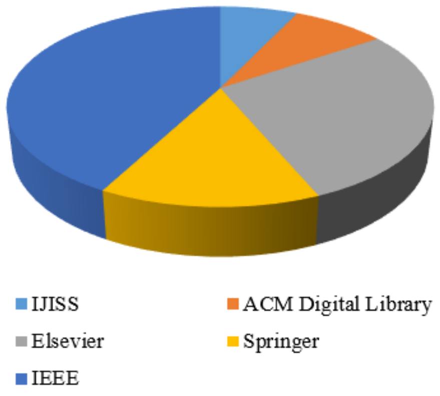

Figure 5. Percentage of published articles

11. FUTURE RESEARCH DISCUSSION

Future research endeavors aimed at strengthening data security in cloud storage and addressing the evolving challenges and demands of a dynamic digital landscape. In Table 1, the discussions are mainly about the elementary concepts, security features, and efficiency parameters. While considering security parameters, cryptographic algorithms give major importance. A survey about some cryptographic algorithms is given in Table 1. Security features include secrecy, integrity, authentication, authorization, confidentiality, reliability, and privacy. From studies [27-32], cost efficiency is measured. Among these [30, 31] is the linear system. Also, while considering all these techniques, authentication is a preferable parameter for improving security. So in the future, all schemes must consider authentication as an efficient parameter for better work. The survey provided insights into the current landscape of cybersecurity practices among businesses, shedding light on both strengths and areas for improvement in securing organizational assets against cyber threats.

Based on software-defined networking (SDN) development, cloud services can be ordered more effectively in security. The system convention permits control of the system applications and gadgets in SDN [54]. The programmability, centralization, and automation capabilities of SDN, cloud environments can significantly enhance their security posture. In addition to SDN, the general idea of cross-storage is applying a server farm [55]. With respect to the idea of bringing together in SDN, storage services could be made reduced complexity and enhance efficiency. Some illustrations include multi-cloud, hybrid cloud, meta-cloud and cloud organizations in the cross-storage [56]. Due to this result, numerous CSP titans like IBM and Microsoft are taking a cross-cloud shot and demonstrating the future course of cloud storage.

Artificial Intelligence (AI) and ML are the main future pattern of the cloud [57, 58]. AI and ML are utilized in cloud storage; the works have demonstrated some primer outcomes in the early stages. Google's AlphaGo is one illustration of AI and utilizes profound learning and different strategies in the AI table. Additionally, the frameworks like Siri from Apple and Cortana from Microsoft are likewise items examined in ML and AI. The method of checking enormous amounts of information in the cloud may change in the future, and in this manner, the future pattern of cloud storage is the ascent of ML and AI. By leveraging AI/ML capabilities, cloud storage security can evolve beyond traditional rule-based systems, enabling proactive threat detection, adaptive response mechanisms, and improved overall resilience against sophisticated cyber threats. Utilizing AI and ML in cloud storage improves security and dependability in a cloud environment [59].

Cloud-to-cloud reinforcement is reinforcement by duplicating it to another cloud. Indeed, even with numerous recuperation advancements created, if only the data is stored without the backup, it cannot retrieve the data. At the same time, it is affected by disasters such as fire or flood. The cloud-to-cloud reinforcement makes more copies repudiated with reduplication advances, including Proof of Work (PoW). Additionally, the investigation is expected to permit an anchored cloud-to-cloud reinforcement. Cryptographic methods, protocols, and access control models can significantly contribute to strengthening security measures, ensuring data confidentiality, integrity, and availability in evolving technological landscapes. Cloud security will be extensively enhanced later on. As they rise the same number of new advancements to incorporate with the cloud, the receptiveness idea of the cloud ought to be the advantages yet also progress toward becoming dangers to its clients. Anything open is unreliable as anybody likewise approaches it, including pernicious clients like programmers. In the field of cloud security, AI and ML can give better performance in cloud storage [59].

Security is important in cloud storage since it is necessary for the growth of cloud storage. Cloud storage users have a lot of fear in case of storage availability issues, security threats and data loss. Nowadays, learning-based methods like ML and AI for security [60] applications are increasing in popularity through the arrival of many techniques. However, the significant issue in these techniques is collecting unbiased and real-time datasets. Many datasets are internal and are not sent because of security problems or the absence of some statistical features. To advance the field effectively, the development of standardized datasets and evaluation benchmarks should be an ongoing collaborative effort involving stakeholders from academia, industry, and regulatory bodies. These approaches are needed for the user to generate a database with the training and testing strategies with the simulated evaluation of experimental evaluation [61]. ML models trained through some single dataset usually produced a semantic gap between applications and the results. It lacks research; it proves the efficiency of these systems and the more datasets acquired in many environments. So ML and AI are important to test ML robustness, specifically in various conditions established in cloud scenarios [62]. These challenges requires a comprehensive approach involving technological advancements, collaborations among stakeholders, robust regulatory frameworks, and ongoing research and innovation to enhance AI/ML systems' capabilities in the realm of security.

The capabilities of quantum cryptography and blockchain, cloud security can be significantly strengthened, offering robust protection against evolving cyber threats and ensuring the integrity, confidentiality, and availability of data stored and transmitted within cloud environments.

Expanding the survey's scope to encompass these areas could provide a more comprehensive understanding of cybersecurity practices across diverse industries and aspects, offering valuable insights for both researchers and practitioners in enhancing organizational cybersecpossurity measures.

12. CONCLUSION

This paper is surveying the cryptography technique, like two-factor data security protection in cloud storage. The paper published from 2000 to 2018 is considered for this survey. It gives more details about the two-factor data security protection for researchers. The background information on cloud storage is provided with the analysis of recent reviews of cloud security. Various cloud storage model is discussed with various security issues for real-time usage. Then the details of two factor security scheme are suggested with the Yubicrypt file specification. The comprehensive analysis of the latest research approaches or algorithms is related to two factor data security protection in cloud storage. Finally, Each of these scopes aims to strike a balance between minimizing interaction time and enhancing security by leveraging automation, advanced authentication methods, continuous monitoring, and proactive threat response strategies. Addressing these research questions can advance the understanding and development of security measures that balance minimized interaction time with robust protection against threats and attacks in various technological environments. This SLR covers several studies of cloud security issues, risk mitigation strategies, cloud security models, and the solution with 2FA. However, the work is restricted to conference and journal papers on ML in cloud security. With the search approach strategy, a vast amount of non-relevant research papers are excluded.

REFERENCES

[1] Wang, C., Ren, K., Lou, W., Li, J. (2010). Toward publicly auditable secure cloud data storage services. IEEE Network, 24(4): 19-24. https://doi.org/10.1109/MNET.2010.5510914

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4): 50-58. http://doi.acm.org/10.1145/1721654.1721672

[3] Subashini, S., Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1): 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[4] Almorsy, M., Grundy, J., Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107. https://doi.org/10.48550/arXiv.1609.01107

[5] Li, Y., Gai, K., Qiu, L., Qiu, M., Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387: 103-115. https://doi.org/10.1016/j.ins.2016.09.005

[6] Zhou, L., Varadharajan, V., Hitchens, M. (2015). Trust enhanced cryptographic role-based access control for secure cloud data storage. IEEE Transactions on Information Forensics and Security, 10(11): 2381-2395. https://doi.org/10.1109/TIFS.2015.2455952

[7] Buyya, R., Ranjan, R., Calheiros, R.N. (2010). InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services. In: Hsu, CH., Yang, L.T., Park, J.H., Yeo, SS. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2010. Lecture Notes in Computer Science, vol 6081. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13119-6_2

[8] Hilley, D. (2009). Cloud computing: A taxonomy of platform and infrastructure-level offerings. Georgia Institute of Technology, Technical Report, 44-45.

[9] Dikaiakos, M.D., Katsaros, D., Mehra, P., Pallis, G., Vakali, A. (2009). Cloud computing: Distributed internet computing for IT and scientific research. IEEE Internet Computing, 13(5): 10-13. https://doi.org/10.1109/MIC.2009.103

[10] Cannon, D.M., Martin, H.N. (2000). Storage management system with file aggregation and space reclamation within aggregated files. United States patent US 6,021,415.

[11] Hanaoka, Y., Hanaoka, G., Shikata, J., Imai, H. (2005). Identity-based hierarchical strongly key-insulated encryption and its application. In: Roy, B. (eds) Advances in Cryptology - ASIACRYPT 2005. ASIACRYPT 2005. Lecture Notes in Computer Science, vol 3788. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11593447_27

[12] Kacker, R.R., Appenzeller, G., Pauker, M.J., Spies, T. (2006). Identity-based encryption system for secure data distribution. United States patent US 7,003,117.

[13] Mowbray, M., Pearson, S. (2009). A client-based privacy manager for cloud computing. In Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and Middleware, pp. 1-8. https://doi.org/10.1145/1621890.1621897

[14] Thakur, J., Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. International Journal of Emerging Technology and Advanced Engineering, 1(2): 6-12.

[15] Liu, J. K., Liang, K., Susilo, W., Liu, J., Xiang, Y. (2015). Two-factor data security protection mechanism for cloud storage system. IEEE Transactions on Computers, 65(6): 1992-2004. https://doi.org/10.1109/TC.2015.2462840

[16] Boren, S.L., Brisson, A.J. (2015). Dynamic distributed key system and method for identity management, authentication servers, data security and preventing man-in-the-middle attacks. United States patent US 9,166,782.

[17] Hanaoka, G., Hanaoka, Y., Imai, H. (2006). Parallel key-insulated public key encryption. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds) Public Key Cryptography - PKC 2006. PKC 2006. Lecture Notes in Computer Science, vol 3958. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11745853_8

[18] Matsuo, T. (2007). Proxy re-encryption systems for identity-based encryption. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds) Pairing-Based Cryptography – Pairing 2007. Pairing 2007. Lecture Notes in Computer Science, vol 4575. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-73489-

5_13

[19] Libert, B., Vergnaud, D. (2008). Unidirectional chosen-ciphertext secure proxy re-encryption. In: Cramer, R. (eds) Public Key Cryptography – PKC 2008. PKC 2008. Lecture Notes in Computer Science, vol 4939. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-78440-1_21

[20] Wang, B., Qi, Z., Ma, R., Guan, H., Vasilakos, A.V. (2015). A survey on data center networking for cloud computing. Computer Networks, 91: 528-547. https://doi.org/10.1016/j.comnet.2015.08.040

[21] Soares, L.F., Fernandes, D.A., Freire, M.M., Inácio, P.R. (2013). Secure user authentication in cloud computing management interfaces. In 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, pp. 1-2. https://doi.org/10.1109/PCCC.2013.6742763

[22] Lang, J., Czeskis, A., Balfanz, D., Schilder, M., Srinivas, S. (2017). Security keys: Practical cryptographic second factors for the modern web. In: Grossklags, J., Preneel, B. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science(), vol 9603. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54970-4_25

[23] Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, pp. 553-567. https://doi.org/10.1109/SP.2012.44

[24] Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., Christin, N. (2018). "It's not actually that horrible" exploring adoption of two-factor authentication at a university. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1-11. https://doi.org/10.1145/3173574.3174030

[25] Das, S., Dingman, A., Camp, L.J. (2018). Why Johnny doesn't use two factor a two-phase usability study of the FIDO U2F security key. In: Meiklejohn, S., Sako, K. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science(), vol 10957. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-58387-6_9

[26] Das, S., Russo, G., Dingman, A.C., Dev, J., Kenny, O., Camp, L.J. (2018). A qualitative study on usability and acceptability of Yubico security key. In Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust, pp. 28-39. https://doi.org/10.1145/3167996.3167997

[27] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. IEEE Access, 9: 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203

[28] Abdulsalam, Y.S., Hedabou, M. (2021). Security and privacy in cloud computing: technical review. Future Internet, 14(1): 11. https://doi.org/10.3390/fi14010011

[29] Jebali, A., Sassi, S., Jemai, A. (2021). Secure data outsourcing in presence of the inference problem: Issues and directions. Journal of Information and Telecommunication, 5(1): 16-34. https://doi.org/10.1080/24751839.2020.1819633

[30] Rahmani, M.K.I., Shuaib, M., Alam, S., Siddiqui, S.T., Ahmad, S., Bhatia, S., Mashat, A. (2022). Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): A systematic review. Computational Intelligence and Neuroscience, 2022: 9766844. https://doi.org/10.1155/2022/9766844

[31] Belguith, S., Kaaniche, N., Hammoudeh, M. (2022). Analysis of attribute-based cryptographic techniques and their application to protect cloud services. Transactions on Emerging Telecommunications Technologies, 33(3): e3667. https://doi.org/10.1002/ett.3667

[32] Nassif, A.B., Talib, M.A., Nasir, Q., Albadani, H., Dakalbab, F.M. (2021). Machine learning for cloud security: A systematic review. IEEE Access, 9: 20717-20735. https://doi.org/10.1109/ACCESS.2021.3054129

[33] Rong C, Nguyen ST. Cloud trends and security challenges. In 2011 Third International Workshop on Security and Communication Networks (IWSCN), IEEE, Gjovik, Norway, pp. 1-7. https://doi.org/10.1109/IWSCN.2011.6827710

[34] Zhao, G., Rong, C., Li, J., Zhang, F., Tang, Y. (2010). Trusted data sharing over untrusted cloud storage providers. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, pp. 97-103. https://doi.org/10.1109/CloudCom.2010.36

[35] Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. Information Processing & Management, 59(1): 102744. https://doi.org/10.1016/j.ipm.2021.102744

[36] Onyebuchi, A., Matthew, U.O., Kazaure, J.S., Okafor, N.U., Okey, O.D., Okochi, P.I., Taiwo, J.F., Matthew, A.O. (2022). Business demand for a cloud enterprise data warehouse in electronic healthcare computing: Issues and developments in e-healthcare cloud computing. International Journal of Cloud Applications and Computing (IJCAC), 12(1): 1-22. https://doi.org/10.4018/IJCAC.297098

[37] Vinoth, R., Deborah, L.J., Vijayakumar, P., Gupta, B.B. (2022). An anonymous pre-authentication and post-authentication scheme assisted by cloud for medical IoT environments. IEEE Transactions on Network Science and Engineering, 9(5): 3633-3642. https://doi.org/10.1109/TNSE.2022.3176407

[38] Khalil, I.M., Khreishah, A., Azeem, M. (2014). Cloud computing security: A survey. Computers, 3(1): 1-35. https://doi.org/10.3390/computers3010001

[39] Ahmad, S., Mehfuz, S., Beg, J. (2022). Cloud security framework and key management services collectively for implementing DLP and IRM. Materials Today: Proceedings, 62: 4828-4836. https://doi.org/10.1016/j.matpr.2022.03.420

[40] Khan, I. A., & Qazi, R. (2019). Data security in cloud computing using elliptic curve cryptography. International Journal of Computing and Communication Networks, 1(1), 46-52.

[41] Somani, U., Lakhani, K., Mundra, M. (2010). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In 2010 First International Conference on Parallel, Distributed and Grid Computing (PDGC 2010), Solan, India, pp. 211-216. https://doi.org/10.1109/PDGC.2010.5679895

[42] Alam, I., Kumar, M. (2022). A novel protocol for

efficient authentication in cloud-based IoT devices. Multimedia Tools and Applications, 81(10): 13823-13843. https://doi.org/10.1007/s11042-022-11927-y

[43] Mushtaq, M.S., Mushtaq, M.Y., Iqbal, M.W., Hussain, S.A. (2022). Security, Integrity, and Privacy of Cloud Computing and Big Data. In Security and Privacy Trends in Cloud Computing and Big Data, Taylorfrancis.com, CRC Press.

[44] Rao, R.V., Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. Procedia Computer Science, 48: 204-209. https://doi.org/10.1016/j.procs.2015.04.171

[45] Jayabalan, J., Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing, 164: 152-167. https://doi.org/10.1016/j.jpdc.2022.03.009

[46] Crocker, P., Querido, P. (2015). Two factor encryption in cloud storage providers using hardware tokens. In 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, pp. 1-6. https://doi.org/10.1109/GLOCOMW.2015.7414154

[47] Tourani, R., Misra, S., Mick, T., Panwar, G. (2017). Security, privacy, and access control in information-centric networking: A survey. IEEE Communications Surveys & Tutorials, 20(1): 566-600. https://doi.org/10.1109/COMST.2017.2749508

[48] Wang, S., Ye, J., Zhang, Y. (2018). A keyword searchable attribute-based encryption scheme with attribute update for cloud storage. PloS One, 13(5): e0197318. https://doi.org/10.1371/journal.pone.0197318

[49] Yan, Z., Wang, M., Li, Y., Vasilakos, A.V. (2016). Encrypted data management with deduplication in cloud computing. IEEE Cloud Computing, 3(2): 28-35. https://doi.org/10.1109/MCC.2016.29

[50] Bai, S., Yang, G., Shi, J., Liu, G., Min, Z. (2018). Privacy-preserving oriented floating-point number fully homomorphic encryption scheme. Security and Communication Networks, 2018: 2363928. https://doi.org/10.1155/2018/2363928

[51] Aoudni, Y., Donald, C., Farouk, A., Sahay, K.B., Babu, D.V., Tripathi, V., Dhabliya, D. (2022). Cloud security based attack detection using transductive learning integrated with Hidden Markov Model. Pattern Recognition Letters, 157: 16-26. https://doi.org/10.1016/j.patrec.2022.02.012

[52] David, D.S., Anam, M., Kaliappan, C., Selvi, S., Sharma, D.K., Dadheech, P., Sengan, S. (2022). Cloud security service for identifying unauthorized user behaviour. Computers, Materials & Continua, 70(2): 2581-600. https://doi.org/10.32604/cmc.2022.020213

[53] Hossain, M.A., Al Hasan, M.A. (2022). Improving cloud data security through hybrid verification technique based on biometrics and encryption system. International Journal of Computers and Applications, 44(5): 455-464. https://doi.org/10.1080/1206212X.2020.1809177

[54] Software-defined Networking (SDN) - Definition from What Is. Com, Search SDN, 2017. http://searchsdn.techtarget.com/definition/softwaredefined-networking-SDN 2017.

[55] Raffo D. (2017). Hot Data Storage Technology Trends for 2017, Search Storage. http://searchstorage.techtarget.com/feature/Hot-data-storage technology-trends-for-2017, accessed on 8 Apr. 2017.

[56] Elkhatib, Y. (2016). Defining cross-cloud systems. arXiv preprint arXiv:1602.02698. https://doi.org/10.48550/arXiv.1602.02698

[57] Basile D. 5 huge Trends in Big Data and Storage. The Next Web. https://thenextweb.com/insider/2016/04/01/5-big-data-storage trends watch/#.tnw_FA3yw6Rq. 2017.

[58] Dholakiya P. Five Key Cloud Trends to Look Forward to in 2017: Containers, AI, and More. Cloud Tech News. https://www. Cloud computing news.net/news/2017/feb/03/five-key-cloud-trends-look-forward-2017-containersai-and-more/, accessed on 8 Apr. 2017.

[59] Robb D. Top 10 AI and Machine Learning Data Storage Trends, Enterprise Storage Focum.Com. http://www.enterprisestorageforum.com/storagemanagement/top-10-ai-and-machine-learning-data-storage-trends.html, accessed on 21 Dec 2017.

[60] Bhamare, D., Salman, T., Samaka, M., Erbad, A., Jain, R. (2016). Feasibility of supervised machine learning for cloud security. In 2016 International Conference on Information Science and Security (ICISS), Pattaya, Thailand, pp. 1-5. https://doi.org/10.1109/ICISSEC.2016.7885853

[61] Gadde, S., Amutharaj, J., Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. Journal of Information Security and Applications, 73: 103412. https://doi.org/10.1016/j.jisa.2022.103412

[62] Gadde, S., Amutharaj, J., Usha, S. (2023). Cloud multimedia data security by optimization-assisted cryptographic technique. International Journal of Image and Graphics, 2450010. https://doi.org/10.1142/S0219467824500104