International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183869

# A Review on Biometric based Privacy Preserving and Public Auditing Schemes in Cloud Computing Environment

**Sarita Motghare[1], Dr. C. S. Satsangi[2]**
[1]Research Scholar, CSE, Medicaps University, Indore, Madhya Pradesh, India
[2]Professor, Department of Computer Science and Engineering, Medicaps University, Indore, Madhya Pradesh, India

## ABSTRACT

Cloud technology is very useful for the business development, as it brings about astonishing results in a short time. It is human nature that we trust those things, which are present in front of our eyes. However, in case of cloud computing, the data is mostly outsourced. There always remains a concern for the security and integrity of the data. The privacy of the user is also an important area of concern. Many systems and technique are being developed to address these issues, but still there is always a scope of improvement. While addressing the issues related to the user privacy and data security and integrity, we must consider the efficiency of the system while accessing and searching for the data. In this paper, we discuss about the major challenges in cloud environment. Also, presented is a brief overview on existing research that has been carried out in the above-mentioned areas.

**Keywords :** Cloud Computing, Public Key Infrastructure, Privacy Preserving in cloud, Public Auditing Scheme

## I. INTRODUCTION

Cloud computing is broadly grasped by numerous association and people in view of its different amaze focal points. Different aspects like colossal size data storage, bulky calculation, low-value benefit and adaptable approach to get to the data are considered. The fundamental idea driving cloud computing is virtualization. In cloud computing, virtualization intends to make a virtual variety of a gadget or asset. For example, a server, storage gadget, organize or working system where the structure partitions the asset into the required number of execution conditions. Cloud computing is a dominating administration of cloud storage. It enables data owner to store their data from their nearby computing system to cloud. Numerous clients store their data on cloud storage. Anyway, new convention of data facilitating administration additionally presents security and productivity issue.

One of the primary concern is the rightness and integrity of the data. Once the data is transferred, the data owner would be stress that data could be lost in the cloud. In this manner, the greatest concern is the means by which to decide if a cloud storage system and specialist organization meet the client desires for data security. In this manner, it is vital and noteworthy to increase proficient auditing plan to fortify data owners′ confidence in cloud storage. Different kinds of auditing models have been proposed, they can be sorted into two sorts Private auditing model and Public Auditing Model. Generally, in Private auditing model, data owner can confirm the integrity of outsourced data dependent on the two-party storage auditing convention. In this

method, the data owner ought to have mastery and technical skills. It expands the overhead of data owner and in some cases, it likewise happens the two data owner and CSP cannot persuade each other for the outcome. Thus creating a trust issue that results in false auditing.

The next concern is the security mechanism related to the accessing the data through the cloud. Traditional Key generation mechanism used for encryption is not capable of countering the advance attacks deployed by the attackers. In such a scenario, an encryption method based on user attribute could be an efficient way. It offers a unique key based on a user attribute, which can make the unauthenticated data access very difficult but still there is the definite scope of error. To overcome any such event and hybrid approach of an attribute-based mechanism coupled with user fingerprint can improvise the system. It may overcome the issue unauthenticated data access and can even make it nearly impossible.

Focusing way too much on the security concerns and implementing the resolution for the same can also lead to the degradation in the efficiency. It results in denial of data access by the legitimate user. Thus focusing solely on improving the security measures and ignoring efficiency cannot be a good idea. The system must be secure but the efficiency in the data access and searching of data must be maintained.

In this paper, we present the review on available mechanisms and researches, which in some or other way tried to overcome or counter the above-discussed issues. Firstly, we will cover the researches related to the implementation of biometrics for cloud environment. Then we will discussed about the existing public auditing schemes and try to find out which one could be a better option. After that, we will focus on the encryption and key distribution mechanism with an efficient way to search the data over encrypted environment.

## II. REVIEW OF LITERATURE

Biometric identification has turned out to be progressively in recent times. With the advancement of cloud computing, data owners are persuaded to redistribute the expansive size of biometric data. Identification errands to the cloud to dispose of the costly storage and calculation costs, which, nevertheless, conveys potential dangers to clients' privacy. In this study presented in [1], the author proposes a productive and privacy-saving biometric identification-redistributing plan. In particular, use of biometric to execute a biometric identification. The database owner encodes the data and submits it to the cloud. The cloud performs identification tasks over the database and returns the outcome to the database owner. Here author accept that the biometric data has been handled to such an extent that its portrayal can be utilized to execute biometric coordinate. Without loss of simplification, the system target fingerprints and utilize FingerCodes to speak to the fingerprints. To assess the proficiency and security prerequisites, the author actualizes another encryption calculation and cloud authentication confirmation. The evaluation result and examination indicate it can oppose the potential assaults.

In this study [2], the author proposes a lightweight secure access control conspire for IMDs amid crises. This plan uses patient's biometric data to forestall unauthorized access to IMDs. The plan comprises of two levels: level 1 utilizes some essential biometric data of the patient and it is lightweight; level 2 uses patients' iris data for authentication and it is exceptionally viable. In this exploration, the author additionally makes commitments to human iris check: we find that it is conceivable to perform iris confirmation by looking at halfway iris data instead of the whole iris data. The evaluation aftereffects of

the system demonstrates that the safe access control plot is exceptionally viable. It has little overhead henceforth possible for IMDs. In particular, the false acknowledgment rate (FAR) and false dismissal rate (FRR) of our safe access control conspire are near 0.000% with a reasonable edge, and the memory and calculation overheads are satisfactory.

For security, it is essential that the customer does not pick up anything on the database. The server ought not to get any data about the asked for biometry and the result of the coordinating procedure. The proposed convention in this study [3] pursues a multi-party calculation approach and makes broad utilization of homomorphic encryption as fundamental cryptographic crude. To keep the convention intricacy as low as could be expected under the circumstances, a specific portrayal of fingerprint pictures, named Finger code, is received. In spite of the fact that the past chips away at privacy-saving biometric identification center around choosing the best coordinating character in the database, this arrangement is a nonexclusive identification convention and it permits to choose and report all the enlisted personalities whose separation to the client's FingerCodes is under a given limit. Variations for basic authentication reasons for existing are given. According to the evaluation result, these conventions gain a remarkable data transfer capacity sparing (around 8 to 24%) whenever contrasted and the best past work and its computational many-sided quality is still low and appropriate for down to earth applications.

Here in [4], the author introduces a productive coordinating convention that can be utilized in numerous privacy-preserving biometric identification systems in the semi-fair setting. Our most broad specialized commitment is another backtracking convention that uses the result of evaluating a jumbled circuit to empower productive neglectful data recovery. We additionally present a more effective convention for computing the Euclidean separations of vectors and streamlined circuits for finding the nearest coordinate between points held by one gathering and an arrangement of focuses held by another. For evaluation reason, usage of a down to earth privacy-safeguarding fingerprint coordinating system is been finished. The fundamental downside is that present conventions for privacy-protecting calculations are extremely costly and unfeasible for genuine scale issues. In this work, the author has demonstrated that those expenses can be significantly diminished for an expansive class of biometric coordinating applications by creating productive conventions for Euclidean separation, finding the nearest coordinate, and recovering the related record.

Data sharing turns into an outstandingly alluring administration provided by cloud computing stages in view of its accommodation and economy. As a potential procedure for acknowledging fine-grained data sharing, attribute-based encryption (ABE) has drawn wide consideration. The issue of at the same time accomplishing fine grainedness, high productivity on the data owner's side, and standard data privacy of cloud data sharing in reality still stays uncertain. This paper [5] addresses the testing issue by proposing another attribute-based data sharing plan reasonable for asset restricted portable clients in cloud computing. This plan dispenses with a lion's share of the calculation undertaking by including system public parameters other than moving fractional encryption calculation disconnected. What's more, a public ciphertext test stage is performed before the decryption stage, which disposes of the vast majority of the calculation overhead because of ill-conceived ciphertexts. For data security, a Chameleon hash work is utilized to produce a prompt ciphertext, which will be blinded by the disconnected ciphertexts to get the last online ciphertexts.

Identity-Based Encryption (IBE), which rearranges the public key and endorsement administration at Public Key Infrastructure (PKI), is a critical option in contrast to public key encryption. In any case, one of the primary productivity downsides of IBE is the overhead calculation at Private Key Generator (PKG) amid client disavowal. Here in [6], going for handling the basic issue of identity denial, the author brings re-appropriating calculation into IBE and presents a revocable IBE conspire in the server-supported setting. This plan offloads the vast majority of the key age related activities amid key-issuing and key-refresh procedures to a Key Update Cloud Service Provider, leaving just a consistent number of basic tasks for PKG and clients to perform locally. To accomplished this objective use of a novel plot safe procedure is utilized i.e. utilizing a mixture private key for every client, in which an AND door is included to associate and bound the identity part and the time segment. According to the evaluation results, the system accomplishes consistent effectiveness for both calculation at PKG and private key size at the client. Additionally, User needs not to contact with PKG amid the key refresh, as it were, PKG is permitted to be disconnected in the wake of sending the disavowal rundown to KU-CSP. In addition, finally, no protected channel or client authentication is required amid key-refresh between client and KU-CSP.

This paper [7] endeavours to address the issue of accomplishing productive and solid key administration in secure deduplication. The system presents a gauge approach in which every client holds a free ace key for scrambling the focalized keys and redistributing them to the cloud. Nevertheless, such a gauge key administration plot produces a huge number of keys with the expanding number of clients and expects clients to dedicatedly ensure the ace keys. To this end, the author proposes Dekey, another development in which clients do not have to deal with any keys without anyone else however rather safely appropriate the focalized key offers over various servers. Security examination exhibits that Dekey is secure as far as the definitions determined in the proposed security show.

ABE gives a protected way that enables data owner to share outsourced data on untrusted storage server rather than a confided in server with a predefined gathering of clients. This preferred standpoint makes the strategy engaging in cloud storage that requires secure access control for an extensive number of clients having a place with diverse associations. By the by, one of the principle proficiency drawback of ABE is that the computational expense amid the decryption stage develops with the intricacy of the access recipe. Subsequently, before broadly sent, there is an expanding need to enhance the effectiveness of ABE. To address this issue, outsourced ABE, which gives an approach to redistribute escalated computing assignment amid decryption to CSP without uncovering data or private keys, was presented. Going for wiping out the overhead calculation at both the attribute authority and the client sides, we propose an outsourced ABE plot supporting outsourced decryption as well as empowering delegating key age. In this development [8], the author presents an insignificant arrangement controlled by a default attribute and utilize an AND door associating the inconsequential strategy and client's approach. Amid key issuing, attribute authority can re-appropriate calculation through appointing the assignment of producing a halfway private key for client's arrangement to a key age specialist co-op (KGSP) to decrease neighbourhood overhead. In addition, the outsourced decryption is acknowledged by using key blinding. All the more accurately, the client can send the blinded private key to a decryption specialist co-op (DSP) to perform fractional decryption and do the total decryption at nearby. Following our method, steady effectiveness is accomplished at the two attributes authority and client sides.

Mysterious attribute-based encryption (unknown ABE) empowers fine-grained access control over cloud storage and jelly beneficiaries' attribute privacy by concealing attribute data in ciphertexts. Nevertheless, in existing unknown ABE work, a client knows whether attributes and a concealed arrangement coordinate or not just in the wake of rehashing decryption endeavours. What's more, every decryption as a rule requires numerous pairings and the calculation overhead develops with the many-sided quality of the access recipe. Henceforth, existing plans endure an extreme proficiency downside and are not reasonable for portable cloud computing where clients might be asset compelled. In this study [9], the author proposes a novel procedure called “coordinate then-unscramble”, in which a coordinating stage is also presented before the decryption stage. This method works by computing unique segments in ciphertexts, which are utilized to play out the test that if the attribute private key matches the shrouded access strategy in ciphertexts without decryption. For quick decryption, exceptional attribute mystery key segments are created which permit accumulation of pairings amid decryption. We propose an essential mysterious ABE development and afterward get a security-improved expansion based on emphatically existentially unforgeable one-time marks. In the proposed developments, the calculation cost of an attribute coordinating test is short of what one decryption activity, which just needs a little and consistent number of pairings. Formal security investigation and execution examinations show that the proposed arrangements at the same time guarantee attribute privacy and enhance decryption proficiency for outsourced data storage in portable cloud computing.

This study [10] present a system for acknowledging complex access control of encoded data that we call Ciphertext-Policy Attribute-Based Encryption. By utilizing this strategy, scrambled data can be kept private regardless of whether the storage server is untrusted; also, this technique counters intrigue assaults. Past Attribute-based Encryption, systems utilized attributes to depict the encoded data and incorporated arrangements with client's keys; while in this system, attributes are utilized to portray a client's qualifications, and a gathering scrambling data decides an approach for who can unscramble. Pretty much this technique is adroitly nearer to customary access control strategies, for example, Role-Based Access Control (RBAC).

Apart from secure key distribution and privacy preserving, one of the main challenge is to assure the confidentiality and integrity of the data. At present, there is a significant increment in the measure of data put away in storage administrations, alongside the emotional advancement of systems administration methods. In storage administrations with gigantic data, the storage servers might need to diminish the volume of put away data, and the customers might need to screen the integrity of their data with a minimal effort since the expense of the capacities identified with data storage increment in extent to the span of the data. To accomplish these objectives, secure deduplication and integrity auditing appointment procedures have been contemplated, which can lessen the volume of data put away in storage by taking out copied duplicates and allow customers to effectively check the integrity of put away records by designating expensive activities to a confided in party, individually. The plan displayed in [11] bolsters both secure deduplication and integrity auditing in a cloud situation. Specifically, this plan gives a protected deduplication of scrambled data. The proposed plot additionally bolsters public auditing utilizing a TPA (Third Party Auditor) to help low-fuelled customers. The technique fulfils all essential security prerequisites and is more effective than the current plans that are intended to help deduplication and public auditing in the meantime.

To secure outsourced data in cloud storage against defilements, adding adaptation to non-critical failure to cloud storage together with data integrity checking and disappointment reparation winds up basic. As of late, recovering codes have picked up notoriety because of their lower repair transfer speed while giving adaptation to non-critical failure. Existing remote checking strategies for recovering coded data just give private auditing, requiring data owners to dependably remain on the web and handle auditing, and also repairing, or, in other words. In this paper [12], the author centers around the integrity confirmation issue in recovering code-based cloud storage, particularly with the utilitarian repair methodology. The featuring parts of this study can be outlined by the accompanying angles:

- This system utilizes a novel homomorphic authenticator based on BLS signature, which can be created by two or three mystery keys and confirmed publicly. Using the straight subspace of the recovering codes, the authenticators can be registered effectively. In addition, it very well may be adjusted for data owners furnished with low-end calculation devices (e.g. Tablet PC and so on.) in which they just need to sign the local squares.

- It is the principal plan to permit privacy-protecting public auditing for recovering code-based cloud storage. A PRF (Pseudorandom Function) amid the Setup stage to keep away from spillage of the first data veils the coefficients. This technique is lightweight and does not acquaint any computational overhead with the cloud servers or TPA. Largely, this plan totally discharges data owners from the online weight for the recovery of squares and authenticators at broken servers and it gives the benefit to a proxy for the reparation.

With data storage and sharing administrations in the cloud, clients can undoubtedly change and offer data as a gathering. To guarantee shared data integrity can be checked publicly, clients in the gathering need to register marks on every one of the squares in shared data. Distinctive squares in shared data are for the most part marked by various clients because of data alterations performed by various clients. This paper [13], the author proposes a novel public auditing component for the integrity of imparted data to productive client renouncement at the top of the priority list. By using the possibility of proxy re-marks, the system enables the cloud to leave hinders in the interest of existing clients amid client repudiation with the goal that current clients don't have to download and re-sign squares without anyone else's input. What's more, a public verifier is constantly ready to review the integrity of shared data without recovering the whole data from the cloud, regardless of whether some piece of shared data has been re-marked by the cloud. Besides, our component can bolster clump auditing by confirming different auditing errands at the same time.

Keeping in mind the end goal to address the issue of data integrity over the cloud and further accomplish a safe and reliable cloud storage benefit, the author proposes in this paper [14] an adaptable circulated storage integrity-auditing instrument, using the homomorphic token and appropriated deletion coded data. The proposed configuration enables clients to review the cloud storage with exceptionally lightweight correspondence and calculation cost. The auditing result guarantees solid cloud storage accuracy ensure as well as at the same time accomplishes quick data mistake restriction, i.e., the identification of getting into mischief server. Considering the cloud data are dynamic in nature, the proposed configuration additionally underpins secure and effective unique activities on outsourced data, including square alteration, erasure, and affix.

Cloud computing can gather and redesign a gigantic measure of IT assets and obviously, the cloud servers can give more anchor, adaptable, different, financial and customized administrations contrasted

and the neighbourhood servers. Likewise, to make full utilization of the data on the cloud, the data clients need to access them adaptable and efficient. Therefore, a colossal test of re-appropriating the data to the cloud is the means by which to ensure the classification of the data legitimately while keeping up their accessibility. In this paper [15], a hierarchical attribute-based encryption conspire is first intended for a record gathering. An arrangement of reports can be scrambled together on the off chance that they share a coordinated access structure. Contrasted and the ciphertext-arrangement attribute-based encryption (CP-ABE) plans, both the ciphertext storage space and time expenses of encryption/decryption are spared. At that point, a file structure named attribute-based recovery highlights (ARF) tree is developed for the report gathering based on the TF-IDF show and the archives' attributes. A profundity first looks calculation for the ARF tree is intended to enhance the pursuit effectiveness, which can be additionally enhanced by parallel computing.

Author of this paper [16] addresses the understudied issue for the PPI methods i.e how to give separated privacy protection within the sight of multi-keyword report look. The separation is vital as terms and expressions bear natural contrasts in their semantic implications. In this paper, we present e-MPPI, the principal work to furnish the conveyed report look with quantitatively separated privacy safeguarding. In the plan of e-MPPI, we recognized a suite of difficult issues and proposed novel arrangements. For one, we figured quantitative privacy calculation as an enhancement issue that strikes a harmony between privacy safeguarding and seeks productivity. We likewise tended to the testing issue of secure e-MPPI development in the multi-space data organize which needs common trusts between areas. Towards a safe e-MPPI development with satisfactory execution, we proposed to upgrade the execution of secure multi-party calculations by making a novel utilization of mystery sharing. We executed the e-MPPI development convention with a working model.

## III. REFERENCES


[1] Liehuang Zhu, Chuan Zhang, Chang Xu, Ximeng Liu, And Cheng Huang, “An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing”, Volume 6, IEEE Access March 2018.

[2] XialiHei, Xiaojiang Du, “Biometric-based two-level secure access control for Implantable Medical Devices during emergencies”, in 2011 Proceedings IEEE INFOCOM.

[3] Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, “Privacy-Preserving FingerCodes Authentication”, in Proceedings of the 12th ACM workshop on Multimedia and security, Pages 231-240 , September 2010.

[4] Yan Huang, LiorMalka, David Evans, Jonathan Katz, “Efficient Privacy-Preserving Biometric Identification”,18th Network and Distributed System Security Conference (NDSS 2011), 6-9 February 2011.

[5] Jin Li, Yinghui Zhang, Xiaofeng Chen, Yang Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing”, in computers & security, Volume 72,p 1–12, Elsevier 2017

[6] Jin Li, Jingwei Li, Xiaofeng Chen, ChunfuJia, and WenjingLou,”Identity-Based Encryption with Outsourced Revocation in Cloud Computing”, IEEE Transactions On Computers, Vol. 64, NO. 2, FEBRUARY 2015.

[7] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, “Secure Deduplication with Efficient and Reliable Convergent Key Management”,IEEE Transactions On Parallel And Distributed Systems, Vol. 25, NO. 6, JUNE 2014.

[8] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, "Securely Outsourcing Attribute-Based Encryption with Checkability", IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 8, AUGUST 2014.

[9] Yinghui Zhang , Xiaofeng Chen, Jin Li, Duncan S. Wong, Hui Li, Ilsun You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing",in computers & security, Elsevier 2016.

[10] John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption", IEEE Symposium on Security and Privacy (SP '07),IEEE 2007.

[11] Taek-Young Youn, Ku-Young Chang, Kyung Hyune Rhee, And Sang Uk Shin, "Efficient Client-Side Deduplication of Encrypted Data with Public Auditing in Cloud Storage", IEEE Access 2018.

[12] Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage", IEEE Transactions On Information And Security, Vol. 1 No 2015.

[13] Boyang Wang, Baochun Li, Hui Li, "Panda: Public Auditing for Shared Datawith Efficient User Revocation in the Cloud", IEEE Transactions On Services Computing, Vol. 8, No. 1, January/February 2015.

[14] Cong Wang, Qian Wang, KuiRen, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions On Services Computing, Vol. 5, No. 2, April-June 2012.

[15] Na Wang, Junsong Fu, Bharat K. Bhargava, Jiwen Zeng, "Efficient Retrieval over Documents Encrypted by Attributes in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol13, Issue 10, Oct 2018.

[16] Yuzhe Tang, Ling Liu, "Privacy-Preserving Multi-Keyword Searching Information Networks", IEEE Transactions on Knowledge and Data Engineering, VOL. 27, NO. 9, SEPTEMBER 2015.