Survey of Triangle Security in Cloud

Judy Flava B[1], Ballika J Chelliah[2]

[1,2] *CSE Dept., SRM Institute of Science and Technology, Ramapuram, India*
Email: [1]judyflab@srmist.edu.in, [2]ballikaj@srmist.edu.in

Abstract: Cloud computing remains the world's most demanded development trend. It is one of the most important topic whose application is currently being explored. The distributed storage has been one of the apparent administrations in distributed computing. Instead of providing the engaged worker for conventionally organizated storage, the distributed storage sets various outsider individuals with the knowledge. The customer does not care about any details on various external employees and no one knows exactly where information is spared. The distributed storage supplier asserts that the information can be secured, but no one trusts in it. Security risk is information placed in the plain content configuration over cloud and across the organization. This document offers a method that allows customers to securely store and access data from the distributed storage. It also ensures that neither the distributed storage provider, apart from the verified customer, can get details. This technique ensures the safety and confidentiality of cloud-related information. Another favorite position is that if the cloud provider breaks down, the information of the client remains safe as all information is encoded. Customers must also not stress that cloud providers have illegal access to their data.

***Keywords*: Cloud storage, third party audit, digital security, Encrypted file System**

1. Introduction

At the moment, data protection is one of the most important data frameworks problems. Privacy (confirmation that data are distinctly shared by approved people and associations), honesty (confirmation that the data is real and complete), accessibility (confirmation that the frameworks responsible for conveying, removing and processing data are open to the individual who needs it when needed) and recognizability are the most commonly used security policies (capacity to sequentially interrelate remarkably recognizable substances in a manner that is evident). The problem is even more troubling when a few organisations are cooperating with a company and when the specific data structures in the various repositories are "leaving." We suggest a structure in which the records themselves guarantee their safety, so unregulated resources such as distributed storage could be exchanged along the same lines. In order to achieve autonomous reporting, we insert those security sections inside the record itself (e.g. access control, usage control).Triangle cloud security issues

A. Confidentiality

Secrecy implies assurance of information from unapproved divulgence. It relies upon different factors, for example, encryption strategies, Cloud Service Provider and length of key (in symmetric calculation). Privacy assumes a significant part in distributed computing by safeguarding control on associations' information arranged over various workers

B. Integrity

Honesty of information is the assertion that advanced data are not compromised and have to be obtained or modified by those accepted as such. Properness involves ensuring that knowledge remains consistent, accurate and reliable over its entire life cycle.

C. *Avialablity*

Accessibility is determined as the level of time an application and its administrations are accessible, given a particular time span. One accomplishes high accessibility (HA) when the administration being referred to is inaccessible under 5.25 minutes out of every year, which means at any rate 99.999 % accessibility ("five nines"). HA frameworks are shortcoming open minded frameworks with no single purpose of disappointment; at the end of the day, when a framework part fizzles, it doesn't really cause the end of the administration gave by that component, high accessibility in Clouds stays a major test for suppliers since Cloud foundation frameworks are unpredictable and must address various administrations with various necessities. So as to arrive at a specific degree of high accessibility, a Cloud supplier should screen its assets and conveyed benefits persistently.

2. Credible storage sysytem for cloud

The primary errand of is "A Credible stockpiling sysytem "not just putting away the information just as it needs secret putting away additionally and uprightness of the information would be kept up. To accomplish secrecy and respectability of the information, cryptographic strategies can be utilized to scramble information. Encoded record frameworks (EFS) can be utilized to scramble the customer's information inside the cloud. A scrambled record framework is utilized to encode the client's information, oversee and make

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

keys which are utilized for information encryption and unscrambling .Integrity of the information inside the cloud is created. Conventions are created which guarantee that the customer's information is put away just on confided away workers, duplicated distinctly on confided away workers, and assurance that the information proprietors and other advantaged clients of that information access the information safely. The systemsare dependent on confided in processing stage innovation.

In cloud climate, validation of client is a significant factor, since it ensures that the imparting substance is the one guaranteed. Numerous techniques are being utilized to verify clients in cloud computingenvironment. Single Sign On (SSO), username and secret key, multifaceted validation, Mobile Trusted Module (MTM), Public Key Infrastructure (PKI), just as biometric confirmation are the principle strategies being utilized today.

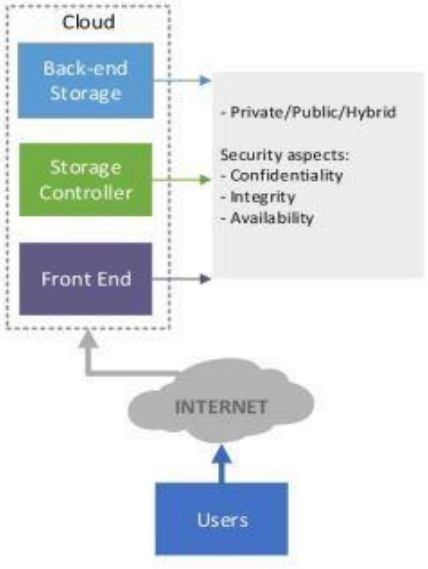

FIGURE 1: CLOUD SECURITY

3. Challenges

A. Risk in Audited -Data Manipulation

The arrangement of the revision by a supplier itself of essential information is a problem for them: the risk of data control. Suppliers can modify the information provided to ensure progressive adherence to the affirmation. Foreshadowing the control or euphemisation of cloud specialist organizations by relevant information is essential to ensure CA is reliable and robust. Suppliers therefore have to create reliable logging systems that fulfill a significant degree of log-on privacy. To achieve that, we can build on findings from the cloud law research area. Cloud legal studies are described as the use of logical standards, creative practices for restoring the past distributed software structures through evidence, assortment, security, evaluation, interpretation and disclosure of computerized evidence [20]. Analysts have proposed different methodology to manage difficulties of cloud criminology (i.e., malignant cloud specialist organizations controlling log records), eventually empowering outsider agents to gather and break down pertinent information [21]. Cloud specialist organisation, to focus log passages and transfer them from different logging sources (e.g. hypervisors), to a focal-logging component [22], will perform appropriate log connectors. In a safe, scratche and consistent log-type, this focused logging section changes log passages. For the prevention of internal log management, an external module (e.g. device or virtual module[21]) that provides a safe capability for log encryption may be updated. Compartative proposals for the use of open source distributed computer stages to guarantee protection and classification of log-based data are suggested (i.e. homomorphic encryption) and evaluated [23], [49]Further on, one method of uncovering information control is to set up a chain of guardianship for computerized proof [25], which speaks to a guide that shows how information was gathered, investigated, and saved so as to be introduced as proof in court. In addition, a few strategies are prescribed to accumulate confided in review significant information, including distant knowledge about confident and stable networks, the use of board aircraft and the preparation of live legal sciences about frames in the running state, as well as an image clone (cf., [21] for an itemized examination). In any event, investigative structures for the cloud crime scene will fluctuate according to the distributed computer management and arrangement model [24]. For example, software-as-a-service and platform models have a restricted authority over cycle or organizational checks, even though some scientifically beneficial logging aspect may be expressed in infrastructure-as-a-Service settings. Future exploration should determine how current cloud review techniques can be used to motivate CA. Workshop participants and customers examined a low likelihood of internal change as continuous change is strong in use. In addition, information management allows a provider to store data volumes multiple times; initial information is unmodified for interior evaluations; and, subsequent information altered for reviewers and customers. At long last, clients may uncover altered information when utilizing the administration (e.g., altered accessibility rate). However, clients just as suppliers suggest that evaluators ought to haphazardly perform approval tests on routinely premise to forestall information control or uncover altered information.

B. Integrity Issues

Giving trustworthiness alludes to guarding data against inappropriate adjustment or pulverization and incorporates guaranteeing data nonrepudiation and validness [76]. With regards to CA, guaranteeing trustworthiness and guarding data against inappropriate adjustment by outer just as inside subjects must be thought of. Aggressors may be keen on

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

focusing on interfaces and frontends to adjust provisioned and introduced information. An alteration of information may influence an evaluator's appraisal of measures adherence, and subsequently may bring about confirmation non-adherence or client disappointment. In like manner, assailants may alter information, which is introduced to clients to demonstrate awful help conduct. Finally, the loss of notoriety or cancelation of the agreements may be prompt in such attack situations. Providers and evaluators therefore need to achieve the highest level of degree for data integrity and develop security instruments.

C. Confidentiality Issues

Guaranteeing classification alludes to Saving authorised access and disclosure limits, including maintaining personal and exclusive data protection [26]. At the point when information is moved to inspectors or introduced to clients, protection of review pertinent information must be guaranteed to forestall spillage of delicate or security-applicable data. Thusly, information must be anonymized or sifted individually. In this sense, suppliers need to unequivocally separate framework checking information and cloud clients' information. Uncovering delicate client information may break administration level arrangements and subsequently lead to monetary remuneration. Additionally, trade of applicable information through utilizing Interfaces enable suppliers or inspectors to update strong and stable information transmission control systems and encryption tools. Assailants may execute wild power or center attacks to recover sensitive information. At long last, giving delicate cloud administration information bears the danger of vindictive evaluators, whomight misuse review pertinent information. Along these lines, inspectors need to demonstrate that information is kept private

D. *Availability Issues*

Guaranteeing accessibility alludes to guaranteeing opportune and dependable admittance to and utilization of data [36]. With regards to CA, accessibility of cloud frameworks and gave interfaces must be guaranteed. To begin with, performing nonstop observing and examining measure (e.g., continuous information social event, examination and collection activities) may have a generous exhibition sway on cloud administrations. In like manner, disappointments in these activities may prompt unsettling influence of cloud administration activity. Subsequently, CA may undermine cloud administration accessibility. Second, when review significant information is given through characterized interfaces, suppliers need to guarantee accessibility of them. Assailants may target interfaces, for instance, by performing disseminated refusal of administration assaults to upset the cycle of CA. In most pessimistic scenarios, this may prompt non-adherence of CSC models, since inspectors are missing comparing review data. At long last, suppliers need to guarantee that gave UIs to clients are accessible

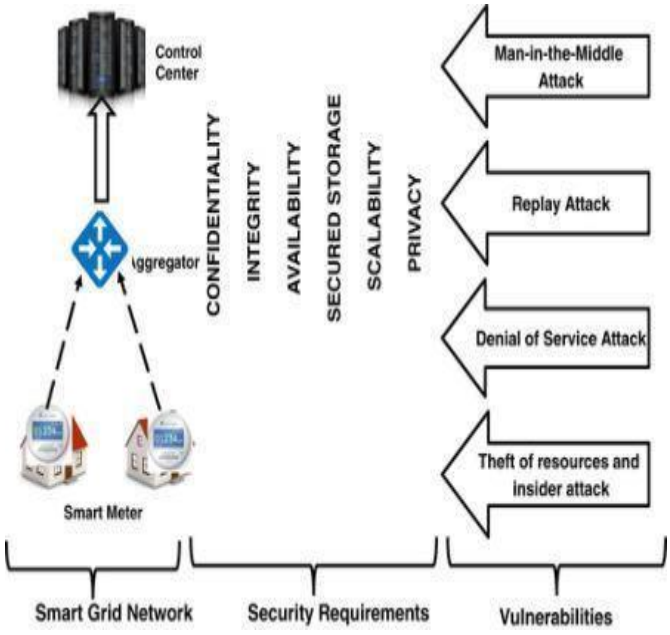

FIGURE 2: CLOUD SECIRITY CHALLENGES

4. Information Security Concerns

The insurance targets incorporate equipment, programming and data. This part chooses three commonplace parts of PC security, including attack forms, access control and encryption. 1) Type of attack: In this section, we summarize several average kinds of attacks, including denial of service (DoS), jack-clicking, listening in, caricaturing, social designing, altering, benefit heightening, and indirect access assaults. Each assault is explicit or vague to the systems administration association layer or operating system.

5. Integrity With Blockchain

A. Verification of Data Integrity in Public

The significant thought of the communal check procedure [33], [34], [35] is that the client (i.e., information proprietor) parts the information into different squares, registers a mark for every one, and redistributes the information obstructs just as relating marks to the cloud worker. The Inspector selects an arbitrary subset of all blocks (i.e. 300 squares of 10,000) and sends the square files (as a complicated signal) to the cloud operator when the information is confirmed to be honest. With the comparison validation, the cloud worker reactions and the examiners verify the honesty of the measured squares by examining the credibility of the examination. The correctness of the entire knowledge index is ensured in the absence of validation. The main strategy here is accumulated mark [39], that enables the examiner, without downloading the details, to confirms different places. After re-appropriating details, the customer sets a check period for open confirmation plans (i.e., the recurrence at which the examiner plays out the confirmation).

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

The examiner would then verify the redistributed correctness of the details at the time of reference. The examiner provides a confirmatory report of different findings from time to time (comparing to numerous periods, we consider these periods an age). If the check result is reject in any time, this means that the information could be contaminated and the inspector must educate the customer on a double basis. Something else, the examiner produces a check log and furnishes the client with the log toward the finish of every age. Since the reviewer can check the information trustworthiness without the client's interest, the client can appoint the inspector to play out the confirmation with any period varying. At the end of the day, from the client's viewpoint, if the re-appropriated information is ruined, the longest deferral inside which she/he needs to discover the information defilement ought to be the check time frame. We stress that the recurrence at which the inspector checks the information trustworthiness would not be extremely high by and by, because of the accompanying reasons. To start with, the reviewer serves various clients all the while. On the off chance that clients require the evaluator to performthe information trustworthiness check with a high recurrence, e.g., playing out the confirmation consistently, the reviewer would bear a substantial correspondence and calculation trouble. Moreover, the higher recurrence to play out the information uprightness confirmation, the more expenses to utilize the reviewer. In an ordinary way, customers will not need the inspector to conduct a reliability check for information in current circumstances. Secondly, a trustworthiness review of information with high recurrence will also cause the cloud worker to have serious problems with confirmation. According to.[37], if security instruments can be incorporated into established cloud frames and the costs are impressive for cloud experts, large parts of the suppliers may not recognize the danger that their Service Level Agreements (SLAs) can have comparable security to ensure access to the management.

B. Tthe vulnerability against procrastinatory auditors of verification schemes

In the greater part of prevailing community check plans [16], [14], [30], reviewers are thought to be straightforward and dependable. This implies that the reviewer would sincerely tail the recommended plots, and plays out the check reliably to, these plans can't avoid malevolent reviewers. The most insignificant assault a noxious reviewer can perform is that it generally creates a decent uprightness report without checking the information honesty to evade the confirmation trouble. To defeat such assaults, the client can review the reviewer's conduct toward the finish of every age. Nonetheless, a more precarious assault actually exists in the component: the evaluator conspires with the cloud worker, and consistently creates inclination testing messages to such an extent that solitary the information blocks which are very much kept up are checked, this abstains from uncovering the information defilement. To oppose this assault, the difficult messages ought not be foreordained by any member. Existing plans [20], [21], [22] use Bitcoin to produce the moving the communications to guarantee the irregularity of tested information blocks, where the inspector removes the hash estimation of the most recent square from the Bitcoin blockchain, and creates the difficult message as per the security boundary and the separated hash esteem. Since in the Bitcoinblockchain the hash estimation of a square produced at a future time is erratic, this guarantees that the reviewer can't create an inclination provoking message to misdirect the client, and empowers the client to proficiently review the evaluator's conduct. Notwithstanding, such instrument is helpless against a dawdling inspector. Expecting the concurred confirmation time frame is 1 day, and an age is multi month (i.e., 30 days), this implies that the reviewer checks the re-appropriated information respectability one time for every day, and the client reviews the examiner's practices one time for each month. In general, the examiner will consistently play confirmation and generate a control report such as clockwork. The test did not occur for a hesitant examiner on the first 29 days and would repeatedly search on the last day, where the challenging messages were sent in every check on the first 29 days 2. Some works[18],[35] and[36] are accepting that inspectors are clear yet inquisitive, but there is no contrast between the suspicions from the point of view of knowledge reliability validation, as the inspectors are not distracted from the endorsed plans. The 30th day could be recovered. In this capacity, the review report only reflects the latest (30th day) state of respect for redistributed material. This is not due to the particular goal of the public check: If the new information is contaminated, the owner of the information will find it within 1 day (i.e., one confirmation period). An obvious agreement against the delaying inspector is for the client to examine the practices of the inspector arbitrarily in time. In any case, before the client reviews the accuracy of examiner's practices, she/he needs to connect with the evaluator to acquire the information that records the reviewer's practices for the inspecting, this adequately offers ascend to fashion the information for the inspector and cloud worker. In that capacity, a tarrying reviewer can pass the client's evaluating by conspiring with the cloud worker. Another direct arrangement is to present a confided in specialist co-op who gives a period stepping administration [33]. After every confirmation, the inspector is needed to inquiry the time-stepping on the data, which is utilized to check the information respectability, and is utilized to be evaluated by the client to demonstrate the rightness of its conduct. This empowers the data to be time-touchy, and along these lines can oppose the dawdling reviewer. By and by, the security of such instruments depend on the security and dependability of the time stamping specialist organization, and the supplier here turns into a solitary purpose of disappointment. Besides, the supplier needs

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

to hold up under weighty correspondence and calculation trouble on account of different clients and evaluators. Thusly, how to oppose the delaying examiner without presenting any believed substance is a difficult issue.

C. In the incompetence of PKI-based public verification schemes

The vast majority of prevailing public check plans are based on the public key framework (PKI), wherever a completely confided in endorsement authority gives the members' testaments, and the reviewer needs to deal with clients' authentications to pick the right open keys for the confirmation. In any case, endorsement the board, which incorporates repudiation, stockpiling, dispersion, and check, is expensive and awkward by and by [18], [28]. Along these lines, eliminating the declaration the executives issue could be financial and great by and by.

6. Literature Survey

Shen, W [1] In this paper, suggest an uprightness review plan focused on characteristics for safe distributed storage that maintains information providing sensitive data storage. Our plan allows others to share and use the records that are placed in the cloud, depending on the condition that the document's sensitive data is secure, and they also use the SSig marking as their character to make sure that their identification name is respectable and that their confirmation is correct. Accept ssk is the private key that creates SSig signature record tag and is maintained by the customer. Our proposal is all the more straightforward and basic under such an assumption. [4] intended to defend the proposal by using a homomorphic undeniable label for the examination of careful shared knowledge. In order to facilitate professional client repudiation,[2] the intermediary resignation suggested a general knowledge integrity strategy to audit the customer's rejection. With Shamir mystery sharing[8], a popular knowledge viability analysis plan has been developed to help customers renouncement. The previously mentioned plots all depend on Public Key Infrastructure (PKI), which causes the impressive overheads from the convoluted declaration the board. To disentangle authentication the executives, Wang et al. [4] proposed a character based distant information honesty examining plan in multicloud capacity. This plan utilized the client's character data, for example, client's name or email address to supplant the public key. Wang et al. [5] planned a novel personality based intermediary situated far off information respectability evaluating plan by acquainting an intermediary with measure information for clients. Yu et al. [6] built a far off information trustworthiness evaluating plan with amazing information protection safeguarding in personality based cryptosystems. Wang et al. [7] proposed a character based information uprightness reviewing plan fulfilling unrestricted secrecy and impetus. Zhang et al. [8] proposed a character based distant information uprightness examining plan for shared information supporting genuine proficient client renouncement. Different perspectives, for example, protection safeguarding authenticators [9] and information deduplication [10] in far off information uprightness examining have additionally been investigated. Notwithstanding, all of existing far off information respectability examining plans can't uphold information imparting to delicate data covering up. In this paper, we investigate how to accomplish information imparting to touchy data stowing away in character based respectability examining for secure cloud storage [12] proposed Another remote information verification plan that supports complete information elements with Merkle Hash Tree. In order to alleviate harm caused by key customer presentation, Yu et al. [13–15] suggested strong remote information respetability review plans based on the key update protocol. [16]. In distributed storage situations, knowledge sharing is an essential application. Wang et al.[17] planned a strategy for protecting the safety of customers by changing the ring mark for secure distributed storage to protect the shares of knowledge. Yang et al. [18] have developed a professional data sharing confidence evaluation strategy to underpin the defense of character and to achieve the users' personality recognition. For distributed computing, Wang et al.[1] have proposed a record-scale system-based ABE conspire. Progressive documents using a coordinated admission structure are encrypted in this scheme. The traits are divided between the ciphertext bits. It does not, however, offer truthful details. It also depends on a single TA that may be deceptive. EntaoLuo et al [2] suggested a radical multi-authority and CB-ABE-based complementary divulgation. It uses character property sub-sets to keep a strategic distance from single point deception and overhead performance. This job, however, does not provide confidence in facts. CP-ABE conspired by Tran Viet Xuan Phuong et al [1]. The entrance strategy is characterized by an AND-door with trump cards. The strategy of entry is secured by means of a covert chip text. The main problem of escrow is not resolved, however. YindongChen et al[3] the developer tests the MAC conspires to be upright. In this condition, there is no outsider. Their work is resistant to attacks and assaults from people from the center. There is no repetitive information in their work.

Wang et al [4] The developer proposes a plan to provide safe cloud-based biological framework ensuring information security and safety from customer verification to the disclosure of cloud-based information. The results used in their work are RSA and AES for encryption and scrambling of information, SHA512 and hash bcrypting capacities and HMAC for key administration. Their work offers the benefit of both symmetric and lopsided encryption to the hybrid cryptographic system (HCS). The developer uses the ChainFS system that secures the cloud capacity using blockchain,

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

QiwuZou, Yuzhe et al.[5]. On Ethereum and S3Fs ChainFS is executed with customers based in Fuse, and storage that is additionally distributed through Amazon S3 is also evaluated in the ChainFS system and also demonstrated with a low overhead. ChainFS requires a client, a worker who has a cloud supervision and blockchain facilitation. Customers from Breaker work together on two planes with remote meetings. After verifying the use of the Merkle verification peruse activity is transmitted, and new root hash is used instead of the nearby state generated before it is sent. The intermediate web server loop between the FUSE-blockchain is terminated in ChainFS, where the breaker customer requests the CURL of a web server. In the execution of a hash job here, SHA256 calculation is used. After record creation and the execution of the document read, Framework performance is tested.

J. Yu et al[8] introduced a strong revision for stable distributed storage in 2017, with a proposal for strong key implementation. The strategy uses a competent key updating process and the key presentation does not affect the safety of the exam in other timeframes in a single time period. The TPA creates an update message each time it sends it to the customer, particularly in a specific way. By using the private key and upgrades post, the customer refreshes the mystery key. If the key is not uncovered, the harmful cloud cannot get the markup mystery key. Moreover, at first the details re-appropriated should not be fixed. Whatever the case, the proposal does not maintain community evaluation or information elements that have more space for further review. Zhang et al. [16] proposed a public confirmation conspire for the distributed storage utilizing indistinctness obscurity. Vagary confusion is uses to ensure protection and reduce the evaluator hand, which is the point of the strategy, overhead postponement and measurement. The evaluator does not have a strong calculation capability to verify the correctness of information and is only enough to enter a MAC tag. The cloud is designated for most calculations. The plan is expanded to support cluster monitor and complex knowledge tasks that use the technique of the Merkle hash tree. The assessor can handle different orders from various customers simultaneously and customers can refresh their redistributed details. While the overhead calculation is directly with the size of the information index tested, the overall calculation is not the size of the information index in the plan. On the other hand, the muddled software is not generated by clients and the jumbled Program is not carried out by cloud staff. The proposal cannot stop malicious auditors, in addition. Holy Mother Aldossary et al. According to the creators, the correctness of the information, but also of the opposition, should be tested. Computational confidence refers only to licensed applications, so that the information can be accessed and used for calculation. Any irregularities arising from normal registration should be avoided. A effective Identity and Access Management (IAM) will keep the classification and respectability of the project strategically remote. Accessibility losses can occur by loss of information and unavailability. Distributed computing uses hardly any approach such as simplicity and high design usability. Different policies and methods are adopted to enhance the protection of information classified by three CIA levels in different stages of the cycle of information. Encrypt information if the information is very still and if the information is still on the way. Apart from the Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) strong encryption computation. Various types of methods of encryption. In general, encryption techniques provide confidentiality against attacks by a cloud provider, but information cannot be secured against design errors and programming bugs. Inadvertent and purposeful changes in information can be discovered using hash techniques. In any event, they burn more power and tedious data transfer. External audits can be used to verify the correctness of details.

Liu H et al [19] They suggested the mapping of convention and characteristic admittance control instrument, which are based on mutual authority security. This construction is based on the bilinear matching technique and on the concept of number hypotheses, which is responsible for the high computational costs. The classification of information can also be achieved through an open key system in which each customer wills his character, a public coding key and a private coding key. Due to the bilinear mixing strategy and the complexity of every customer's endorsement which results in high computing costs. [10] Debnath et al. The goal is to represent each cloud administration exchanging the data inside the cloud that can lead to privacy disclosure issues. The issue of confidentiality is mainly opened or spread through cloud administrations for a customer or a business. The center planned a number of secret security plans using blockchain.

7. Conclusion

There are various areas discussed in this article. Presentation, the highlights and circumstances in distributed computing. Writing audits as basis function in distributed computing, problems with cloud, traditional security plans The imaginative novel ultimately suggested responses to these questions. This study shows that no legitimate arrangement is available covering all cloud layers. Many of the existing creators concentrated on the protection of their cloud management clients and not the security of suppliers. All problems in the cloud layers would appear in a single arrangement in this proposition. Privacy, integrity and authentication of data were the key factors in determining the efficient use of our hybrid blockchain algorithm used in the infrastructure. Users can access their private keys as one of the key system deliverables and user data is well formed, transparent and authenticated to protect against threat to a data center. In addition, encrypted data is held away from the hands

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

of cloud vendors or attackers, and data confidentiality is maintained when verification has been carried out by cloud auditors on a decentralized network. In protecting privacy within the cloud and in balance the requirements of the customer and the service provider, the proposed architectures plays an important role. It show the use of decentralization in comparison with previous research in effects to efficiency. The framework therefore underlines the emerging activities within the cloud infrastructure layer and paves the way for a standard scale of privacy for consumers and companies in order to create a higher degree of trust with third parties in order to ensure long-term storage data reliability.

References

[1] Shen, W., Qin, J., Yu, J., Hao, R. and Hu, J., 2018. Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. *IEEE Transactions on Information Forensics and Security*, *14*(2), pp.331-346.

[2] Zhang, Y., Xu, C., Lin, X. and Shen, X.S., 2019.Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Transactions on Cloud Computing.

[3] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "Npp: A new privacy-aware public auditing scheme for cloud data sharing with group users," IEEE Transactions on Big Data, 2017. [Online]. Available: DOI:10.1109/TBDATA.2017.2701347

[4] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, Jan.-Feb. 2015.

[5] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA - Volume 01, ser. TRUSTCOM '15, 2015, pp. 434–442.

[6] H. Wang, "Identity-based distributed provable data possession in multicloud storage," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328–340, 2015

[7] H. Wang, D. He, and S. Tang, "Identity-based proxyoriented data uploading and remote data integrity checking in public cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.

[8] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, April 2017.

[9] H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," IEEE Transactions on Services Computing, 2016.[Online]. Available: DOI: 10.1109/TSC.2016.2633260

[10] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386–2396, Aug 2016

[11] J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure data deduplication with dynamic ownership management in cloud storage," IEEE Trans. on Knowl. and Data Eng., vol. 28, no. 11, pp. 3113–3125, Nov. 2016.

[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.

[13] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.

[14] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016.

[15] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.

[16] J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusion-resilient identity-based signatures: Concrete scheme in the standard model and generic construction," Information Sciences, vol. 442-443, pp. 158 – 172, 2018.

[17] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302.

[18] Shulan Wang, Junwei Zhou,Joseph K. Liu,Jianping Yu, Jianyong Chen, and Weixin Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, VOL. 11, Issue 6, June 2016.

[19] Entao Luo, Qin Liu and Guojun Wang, "Hierarchical MultiAuthority and Attribute-Based Encryption Friend Discovery Scheme in Mobile Social Networks",IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 9, SEPTEMBER 2016

[20] YindongChen, LipingLi, ZiranChen (2017)," An Approach to Verifying Data Integrity for Cloud Storage", IEEEChao

[21] Yangt, Shiyuan Chet, Xueting Cao, Yeqing Sun, Ajith Abraham, "A Rough-Fuzzy C-Means Using Information Entropy For Discretized Violent Crimes Data", I3th International Conference On Hybrid Intelligent Systems (His),2013.

[22] Akshay Arora,Abhirup Khanna, Anmol Rastogi, Amit Agarwal (2017), "Cloud Security Ecosystem for Data Security and Privacy", IEEE..

[23] QiwuZou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, (2018),IEEE 11th International Conference on Cloud Computing ,ChainFS: Blockchain-Secured Cloud Storage.

[24] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, 2017.

[25] Y. Zhang, C. Xu, X. Liang, et al., "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[26] S. Aldossary and W. Allen. Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. International Journal of Advanced Computer Science and Applications, Vol. 7, 2016, No. 4.

[27] Liu, H., Ning, H., Xiong, Q., Yang, L.T.: Shared authority based privacy-preserving authentication protocol in cloud computing. IEEE Trans. Parallel Distrib. Syst. 26(1), 241–251 (2015)

[28] Debnath, A., Singaravelu, P., Verma, S.: Privacy in wireless sensor networks using ring signature. J. King Saud Univ. Comput. Inf. Sci. 26(2), 228–236 (2014)

[29] J. R. Rajalakshmi, M. Rathinraj, and M. Braveen, "Anonymizing log management process for secure logging in the cloud," in Proc. Int. Conf. Circuit, Power Comput. Technol., India, 2014, pp. 1559– 1564.

[30] S. Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS," in Proc. 8th ACM SIGSAC Symp. Inform.,Comput. Commun. Security, Hangzhou, China, 2013, pp. 219–230.

[31] C.-H. Lin, C.-Y.Lee, and T.-W. Wu, "A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics," Int. J.Security Its Appl., no. 2, p. 241, 2012.

[32] Timraz, K., Barhoom, T. and Fatayer, T., 2019, March.A Confidentiality Scheme for Storing Encrypted Data through Cloud. In 2019 IEEE 7th Palestinian International Conference on Electrical and Computer Engineering (PICECE) (pp. 1-5). IEEE.

[33] Arockiam, L. and Monikandan, S., 2014, January. Efficient cloud storage confidentiality to ensure data security.In 2014 International Conference on Computer Communication and Informatics (pp. 1-5).IEEE.

[34] Zhang, Y., Xu, C., Lin, X. and Shen, X.S., 2019.Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Transactions on Cloud Computing.

[35] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Trans. Information Forensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[36] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.

[37] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, and M. Guo, "Making big data open in edges: A resource-efficient blockchain-based approach," IEEE Trans. Parallel and Distributed Systems, to appear, doi: 10.1109/TPDS.2018.2871449.

[38] Wang, Q., Lv, G. and Sun, X., 2019, June. Distributed Access Control with Outsourced Computation in Fog Computing. In 2019 Chinese Control And Decision Conference (CCDC) (pp. 2446-2450). IEEE.

[39] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J. Liu, Y. Xiang, and R. Deng, "Crowdbc: A blockchain-based decentralized framework for crowdsourcing," IEEE Trans. Parallel and Distributed Systems, to appear, doi: 10.1109/TPDS.2018.2881735.

[40] Y. Zhang, C. Xu, H. Li, and X. Liang, "Cryptographic public verification of data integrity for cloud storage systems," IEEE Cloud Computing, vol. 3, no. 5, pp. 44–52, 2016.

[41] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Transactions on Dependable and Secure Computing, 2018. [Online]. Available: DOI:10.1109/TDSC.2018.2829880

[42] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, andR. Hao, "Remote data possession checking with privacypreserving authenticators for cloud storage," Future Generation Computer Systems, vol. 76, no. Supplement C, pp. 136 – 145, 2017.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731