JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Development of Model of Merkel Tree based Key Management in the Cloud Computing

Dr.Harsh Lohiya [1] , Dr. Laxmaiah Mettu[2] , Dharavath Nagesh[3]

[1]Research Guide, Dept. of Computer Science and Engineering Sri Satya Sai University of Technology and Medical Sciences, Sehore Bhopal-Indore Road, Madhya Pradesh, India.

[2]Research Co-Guide, HOD. Dept. of Computer Science and Engineering CMR Engineering College, Kandlakoya (V), Medchal, Hyderabad

[3]Research Scholar, Dept. of Computer Science and Engineering Sri Satya Sai University of Technology and Medical Sciences, Sehore Bhopal-Indore Road, Madhya Pradesh, India.

Abstract

Many businesses store and handle data on the cloud for a variety of purposes. Client information transfers in the cloud are less secure because of the patchy cycle of information uprightness checks. To improve the security of cloud data, this study recommends an improved Merkle Hash Tree technique for successful authentication models in multi-owner clouds. To mix large amounts of data, the Merkle Hash Tree uses leaf hubs with hash tags and non-leaf hubs with databases of child hash data. Merkle hash trees provide effective information planning and, through good design, correctly identify the history of information. The methodology created allows us to maintain open access security and provide a trusted cloud storage infrastructure. Data is sent from the owner to the cloud and processed using private keys. The data is clustered and saved on the cloud server using an improved Merkle hash tree method. The information records provided by the information proprietor are examined by an outside inspector, and the client is verified during the change interaction using the multi-owner authentication approach. Authorities who are rethinking information use have successfully increased their use of information, bringing security and protection concerns to light. Information authentication plays a crucial role in the ability to evaluate advanced content and safeguard it from being altered by internal or external attackers.

Keywords: *Merkel Tree, Key Management, Cloud Computing, Authentication, Motivation, CPABE*

1. Introduction

Many organisations have used cloud computing to store and manage information in a productive manner, and Due to its advantages of adaptability, adaptability, and constant quality, cloud computing is preferred by all organisations. Cloud administrations are the greatest choice for corporations because of their best reaction and adaptability (Aldeen, 2019). The client reassigns the information to store and handle it because of the cloud's elasticity and flexibility. Clients have the option of encrypting their data before sending it to the cloud, and cloud service providers (CSPs) are responsible for maintaining the security of sensitive information. Large, medium, and small businesses use cloud computing to provide virtual computing such as

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). You can access the service. Due to increased availability and special improvements, sending cloud servers for capacity and computation is usually a good idea. The cloud is a popular option for computational tasks due to its service, low cost, and power characteristics. Cloud computing frameworks put security at the forefront, and the urgent need to revise existing security decisions is driving the development of innovative solutions. Client access control security is one of the ongoing security concerns in the cloud. Public validation is the process of hiring a trusted third-party auditor (TPA) to validate your cloud data and reduce the burden on your customers. Nevertheless, the TPA may have unnecessary access to sensitive data within the verification system.

A source hub authenticates a collector hub during an authentication cycle. In simple authentication, the beneficiary uses a symmetric key to match the key, and the sender individually composes an encrypted message. As part of our research, we use a strong cryptosystem for cloud authentication. OTP-based authentication, authentication schemes and cryptographic computations, multiple variable-based authentication, and manipulation of unknown hub identities are examples of different kinds of cloud authentication techniques. Cloud-based attacks often result in the loss of personal customer data and the financial interests of the company. An important aspect of cloud management is security. Identifying affected information in the cloud and retrieving previous versions can be done using information reliability techniques. The cloud must support tracking cycles when decrypting encrypted data and securely restoring client information. Another important component of distorted information is appearance. Therefore, a capable cloud approach is needed to manage security, reliability and search of encrypted data. The study recommends a modified Merkle hash tree technique with multi-operator authentication to retrieve data from cloud capacity. An extended Merkle Hash Tree approach is used to perform credibility assessment of critical information within cloud capacity. Each hub in the Merkle hash tree contains information about its position relative to its parent.

Progresses in information and communication technology (ICT) have helped with the shift from local information management to remote information re-appropriating services in response to the increasing expansion in information volume. Although information reevaluating has some benefits in terms of its low cost, quickness, adaptability, and ease of assistance, it also has possible drawbacks that customers can overlook. Reclaiming information in an external capacity requires that the authority dealing with the distant repository has been given power over it. Accidental information losses or breakage are possible because external capacity management may be less cautious than the information owner. Information leaks and mistakes can result in significant financial loss as well as ineffective attempts. They can happen for a variety of reasons, including poor asset management, irresponsible management, and poorly chosen activities. However, some remote capacity specialist co-ops may strive to cover up losses in order to maintain their reputation (D. He, 2012). A method for successfully and productively examining the accuracy of the information stored in a remote vault using the many tactics

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

available for information trustworthiness is becoming increasingly necessary given the problems of information re-appropriating. Merkle trees are a particularly noteworthy verifiable information structure. A test reaction protocol is used to verify information accuracy in light of the Merkle tree. A prover provides a succession of hub values on the way from a leaf hub (randomly selected by a verifier) to the root hub of the tree. While the verifier can save the single incentive for the root hub in the tree, the prover must construct the entire Merkle tree for the confirmed data. In the end, this method just requires the prover to create the proof by using all of the information blocks, and the verifier to store and work on a small number of hash values. Merkle tree-based authentication has been widely adopted to various frameworks, including block chain developments like Bitcoin, due to its simple calculation and low memory requirements. Of particular note is that its productivity increases consistently as the amount of information to be verified increases.

However, when it comes to online authentication, adversarial parties can gather important data from records by repeatedly doing uprightness checks for the same information. In an absurd situation, a snoop who collects authentication data may be able to unlawfully obtain ownership of information kept in a remote warehouse if this method is just used to verify ownership. We examine potential data spillage from Merkle tree-based web-based authetication to reduce this risk. We provide another Merkle tree-based convention that embeds erratic sources each time the evidence age is done in light of a top to bottom analysis. This eliminates data leakage that we have observed, providing consistently dependable internet-based authentication.

2. Literature Review

This section examines the massive and late investigation strategies for cloud information capacity authentication. To support the proposed idea, a brief analysis of the key assumptions and major gaps in the current writing is presented.

Shajina et al. introduced dual authorization rules with two levels of authorization and priority-based access control lists to increase cloud security and adaptability. We worked on cloud security by adopting triple DES calculation as an additional function according to customer's individuality. This security-focused approach protects her customer's identity, and multiple scenarios were used to test the proposed multi-owner cloud her solution (Doshi, 2011). According to the evaluation, the proposed solution has short network time and high cloud security. The method created enables secure and effective integration of information into separate cloud archives. However, the created techniques perform poorly on huge datasets and offer fuzzy information exchange as a compromise.

Anand et al. Elliptic Curve Digital Signature Algorithm (ECDSA) and Extended Elliptic Curve Duffier-Hellman (EECDH) techniques were recommended for joint authentication in the multi-operator cloud. The proposed EECDH technique was used to exchange protected keys with their owners and thwart man-in-the-middle (MITM) attacks. The proposed approach ensures the accuracy of cloud-based data. The effectiveness of this method is enhanced by a character- and feature-based recording approach. In fact, the cloud computing frameworks created have weaknesses, especially in networks that host third-party layers and complex underpinnings.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Profund et al. Enhanced security with cloud-based secure authentication using blockchain technology. Blockchain technology makes it easy for insiders to change their login credentials for authentication cycles. We evaluated the effectiveness and usefulness of the method in the cloud. Using Scyther's formal framework, the proposed method was tested against no-response attacks, disconnected guesses, pantomimes, and denial of service. The results show how successful the proposed approach was in protecting customer data stored in the cloud. Open cloud computing platforms used in engineered authentication mechanisms have been subject to phishing and social engineering scams. Model sanity checks didn't work well because the encryption of the material was unstructured.

Badr et al. introduced an attribute-based cryptographic approach that accesses information in the cloud by considering permissions, cloud servers, information clients, and information owners. The decryption system was chosen by the information owner to reduce computational complexity. A MAC passphrase for data stored in the cloud was created after encryption. Encryption used a distinctive function, decryption required verification. To estimate how well the proposed method can be demonstrated, For key age, the elliptic bend testament free cryptography technique was used. This tactic eliminates the trusted authority and focuses on numerical actions to increase security. When the strategy's security was examined, it became clear that the method was secure. In comparison to current methods, the suggested strategy lowers computational and correspondence costs. Multi-client admission to securely cloud information is anticipated to benefit from further development.

3. Merkle Tree-Based Authentication

A Merkle tree is created from a succession of information blocks, with the value of an inner hub devalued in comparison to the hash value of its offspring and the value of a leaf hub devalued in comparison to the immediate hash value of the next information block (Figure 1). The preimage-obstruction property of the hash capability in the tree growth methodology means it is computationally impossible to locate the preimage of the given hash esteem. Additionally, because this forms a double tree, the highest depth from leaf to root is often dlog2 ne for n information blocks (Greene, 2019). The Merkle tree serves as a verified information structure for successful verification of the web-based material as a result. There are two components, prover P and verifier V, in Merkle tree-based web-based authentication:

• A proponent P is an element that tries to convince the opposite side (the verifier V) that the information is all that is claimed to be true. Instead of sending the complete substance, the prover sends a small portion of obvious data to increase network transmission capacity.

• Verifier V is a further component that seeks to determine whether prover P's argument is sound or not. The verifier typically only maintains the value of the root hub rather than the value of each hub in the Merkle tree in order to save storage requirements.

It is remarkable that the Merkle tree-based web-based authentication standard validates that the prover and verifier possess equivalent data. As a result, it acknowledges that the verifier may have some confidential (i.e., not publicly available) information about the information that needs to be validated, in contrast to public check. Section 5 handles this subject in great detail.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

It is generally guaranteed that key elements with similar information can obtain a similar Merkle tree due to the hardness hypothesis that it is computationally impractical to locate a preimage of a particular hash value in a reasonable amount of time. Simply put, the security of the hash capability being utilised determines the authentication security in the context of the Merkle tree. By doing this, the verifier V just keeps track of the value of the tree's root hub and discards the remaining metadata when the tree is created. However, with each authentication cycle, the prover P is required to produce a series of (different) hash values that result in a root hub value that is identical to the one maintained by the verifier.

The verifier V in the model shown in Figure 1 selects an odd block record (like 1) as a test. The prover P then creates a Merkle tree using the information in the immediate area, followed by delivering the verifier the comparing remarkable kin routes from the passes on to the root hub (i.e., (H1, H2, H34)). The verifier V determines whether the result is indistinguishable from the value of the root hub stored in adjacent capacity after receiving the confirmation reaction and inferring the root worth of the Merkle tree (i.e., H (H (H1, H2), and H3-4)).

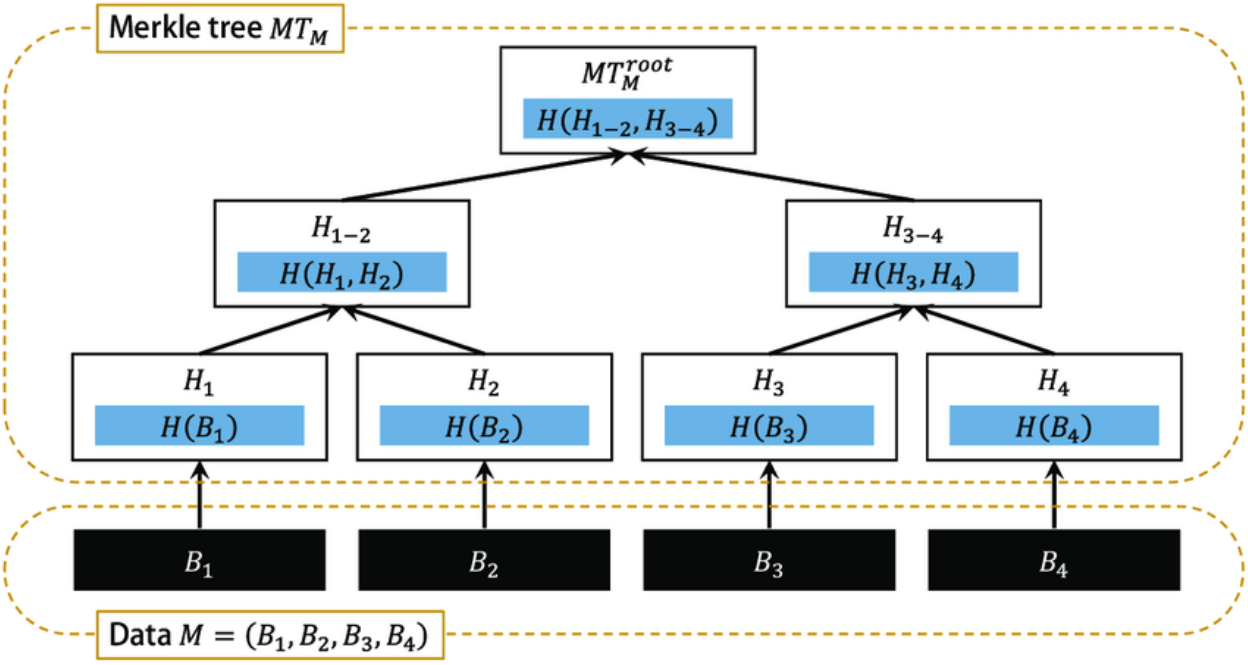


Figure: 1. M Merkle Tree has four blocks of data

As long as a strong (preimage safe) hash capability is used, opponents won't be able to decipher the correspondence's hidden plain information according to the aforementioned convention. In any case, it was found to be vulnerable to side-channel attacks that limit the attack vector by extracting important data from the communication during the authentication cycle, reducing the robustness of the authentication and potentially subverting it. As a result, in Section 3 we first look at how vulnerable Merkle tree-based authentication is to side-channel attacks on data that is similar. Following that, we propose a clear plan for enhancing the security and dependability of Merkle tree-based authentication with negligible above.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

4. Motivation

Patients could use a variety of encoding techniques to further restrict who has access to medical services, making it possible for everyone to understand the patient's more obvious attributes while keeping their more subtle ones hidden. Using CP-ABE, either the entire access strategy with ascribes or just the portion of the strategy that needs to be concealed can be scrambled. In any case, because supported end-clients can access the code text, The framework can't tell whether the end-client has enough permission to access it or not. The previous decoding described cannot be utilised again, which is the second disadvantage of this method. Finally, if the approaches are fully or partially disguised, CPABE encryption alone won't protect the system. In a medical setting where information may be shared across many places, it is essential to make it patient-driven. It might be done by utilising CPABE's fine-grained admittance control and covering the access strategy property at several layers.

4.1. Contributions

Because of the first finding, this focus fundamentally helps develop a Merkle Tree-based admission strategy for delicate attributes in persistently driven information. In our approach, the health credits associated with the information owner (patient) are identified and organized based on kindness and responsiveness. The unimportant, visible highlights contribute right away to the development of a plan. To the free technique, however, is added the root hash of delicate qualities. The code text is only accessible to authorised users, and the security of the sensitive characteristics is maintained.

5. Building the CPABE's suggested Merkle Tree-based Access Structure

By identifying delicate data characteristics over the general access strategy, the underlying goal of our methodology is to provide a Merkle tree-based admission structure for describing access control strategies for patient-centric information. All partners or attributes that have granted access to the PCD are recorded in the entrance tree.

5.1. The System Model

A proposed Merkle tree-based access structure, including confidential attributes such as leaf nodes and public credits in tree TNS, is shown in Figure 1 for the tree TS confidential access approach. The hash root H(TS) of the tree is found and added to the public non-secret tree TNS before sending it to the decrypt or.

Five algorithms are included in our suggested system:

5.1.1. Setup (γ, S) → (PK,MK)

Based on input from and S, the KGC generates PK and MK, respectively.

5.1.2. Key Gen (PK, MK, S) → SK

KGC creates SK for M. PK, MK, and S.

5.1.3. Merkle Tree (TS) Construction of Sensitive Attributes

The Merkle Tree of Sensitive Traits is built with the IBM Clinical Hub in mind. The IBM Clinical Hub provides clinical information items that enable competence, development and access to longitudinal patient records when linked to persistent personality data. IBM Clinical

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Hub provides a more complete workbench model that includes access to patient socioeconomics, clinical information views, and consumption frames and cycles. Longitudinal medical records are produced from his flood of HL7 messages and events related to patient visits, lab orders, results and initiations, clearance and relocation events in a variety of demanding mobile environments. The longitudinal patient record includes information on the patient's prescription, sensitivities, test discoveries, problems, systems, and family history, to name a few things.

5.1.4. Encryption (PK, TNS, TS, M) CT

From the input PK, TNS, TS, and M, TS is the sensitive hash tree, TNS is the public non-sensitive tree, and the sender constructs CT.

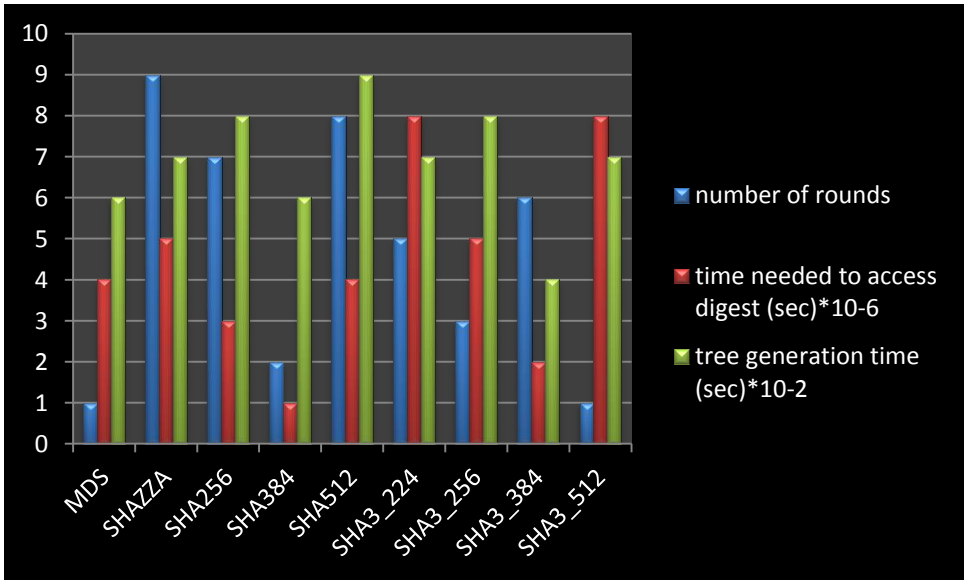
5.1.5. Decryption (CT, SK) M

The Collector, given data sources SK and CT, decodes and produces messages CT and M separately. A Merkle proof can show that a certain quality is available by climbing the hash tree TS from the exchange to the root. During the decryption process, the TNS public tree is verified and Merkle proofs are found, allowing the TS to carefully assess the authenticity of the message based on hidden credits.

6. Results and Discussion

Table: 1. Results

S. No.	Number of Leaf Nodes	Number of Iterations	Leaves Size In Bytes	Internal Nodes' Size (Bytes)
1.	35	36	1255	1565
2.	80	36	4050	5309
3.	156	36	8350	22707



ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

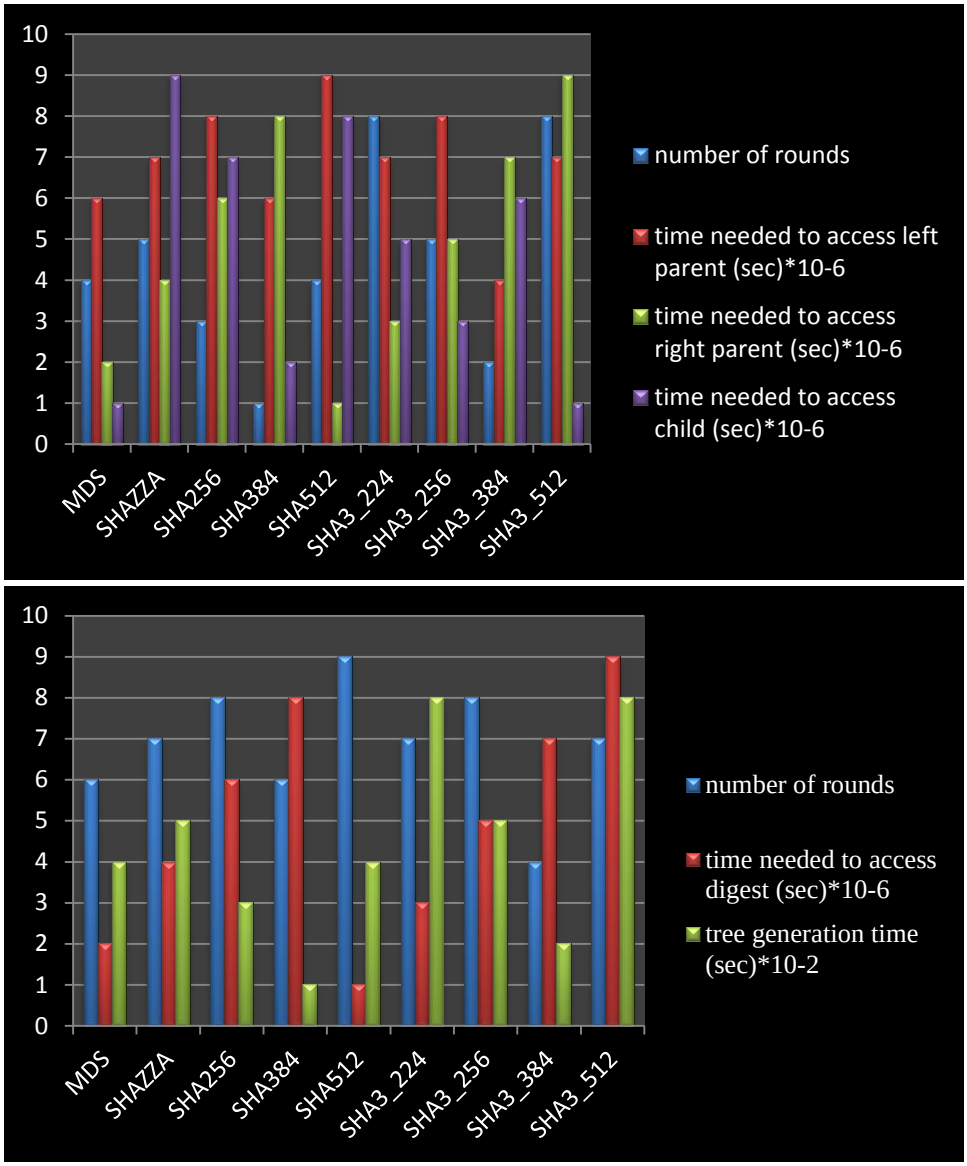


Figure: 2, 3, and 4 The hash calculations are plotted against the times needed to recover the condensate and build the tree in Figures 2, 3, and 4. The third, fifth, and seventh figures are required to reach the child, the right parent, and the left parent, respectively.

6.1. Comparison with different frameworks

In light of the findings in the aforementioned results, we provide a complete correlation that takes into account strategy kind, tree building time, protection safeguarding, information honesty, fine-grained admittance control, and travel time to hubs. We compare the suggested Merkle Tree-based worldview with other novel approaches. Our suggested CP-ABE plot is suitable for carrying out covered touchy trait access procedures since it creates a Merkle tree, ensures trustworthiness using a hashing strategy, and provides fine-grained admittance control.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Table: 2. the proposed model is compared to existing frameworks

Policy Type	Efficiency	Privacy-Preserving	Tree Generation Time	Data Integrity	Time To Access Nodes	Fine-Grained Access Control
conceals sensitive and public access	Low	Y	Moderate	Y	Moderate	Y
No Secret Rules	Low	Y	Moderate	N	Moderate	Y
Only conceals delicate characteristics	Moderate	Y	Less	Y	Less	Y

7. Conclusion

The cloud computing paradigm has become the standard for PC management due to its adaptable processing power and massive storage capacity. In order to further guarantee the security of cloud information capacity, this paper introduces a novel authentication technique. A multi-proprietor authentication method and an improved Merkle hash tree are employed to secure cloud data. Client data is encrypted and stored in the cloud using the improved Merkle hash tree algorithm calculation (Goyal, 2016). The information is recovered using an unscrambling capability in response to a client request. A compelling argument is made for comparing and utilising numerous cloud information capacity authentication methods in the proposed multi-proprietor cloud authentication strategy.

Continuous patient care services typically provide security responses to protect sensitive data and attributes. A Merkle tree-based CP-ABE framework is proposed in this paper. Additionally, it can improve customer and provider trust and security in clinical collaboration and consideration.

Our method allows for the sharing of plans using a uniform access structure and is immune to assaults like plots in the event that an attacker possesses several secret keys. Finally, we show how to apply our framework to other hash types. The security of our architecture must be demonstrated, among other things, utilising a range of static data sources. Massive amounts of data need to be encoded, and work has already begun on producing Merkle evidence that should be quick to produce.

8. References

1. *Aldeen, Y. and Salleh, M., Techniques for Privacy-Preserving Data Publication in the Cloud for Smart City Applications. Smart Cities Cyber security and Privacy, (2019) 129-145.*
2. *D. He, C. Chen, J. Bu, S. Chan, Y. Zhang, and M. Guizani, "Secure service provision in smart grid communications," IEEE Commun. Mag., vol. 50, no. 8, pp. 53–61, Aug. 2012.*
3. *Doshi, N. and Jinwala, D. Constant Cipher text Length in Multi-Authority Cipher text Policy Attribute Based Encryption. 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011),*
4. *Goyal, V., Pandey, O., Sahai, A. and Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security - CCS '06, (2006).*

5. *Greene, E., Proctor, P. and Kotz, D. Secure sharing of mHealth data streams through cryptographically-enforced access control. Smart Health, 12 (2019) 49-65.*
6. *H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484–494, 2017.*
7. *H. Liang, B. Choi, A. Abdrabou, W. Zhuang, and X. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," IEEE J. Sel. Areas Commun., vol. 30, no. 6, pp. 1061–1074, Jul. 2012.*
8. *H. Liang, B. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for PHEVs via V2G system," in Proc. IEEE INFOCOM, 2012, pp. 1674–1682.*
9. *Helil, N. and Rahman, K. CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy. Security and Communication Networks, (2017) 1-13.*
10. *M. Abdel-Basset, M. Mohamed and V. Chang, "NMCDA: A framework for evaluating cloud computing services," Future Generation Computer Systems, vol. 86, pp. 12–29, 2018.*
11. *Meng, F., Cheng, L. and Wang, M. ABDKS: Attribute-Based Encryption with Dynamic Keyword Search in Fog Computing. Frontiers of Computer Science, 15(5) (2021).*
12. *Meng, F., et.al. Ciphertext-Policy Attribute-Based Encryption with Hidden Sensitive Policy from Keyword Search Techniques in Smart City. EURASIP Journal on Wireless Communications and Networking, 1 (2021).*
13. *Nishide, T., Yoneyama, K. and Ohta, K. Attribute-based encryption with partially hidden encryptor-specified access structures | Proceedings of the 6th international conference on Applied cryptography and network security, (2022).*
14. *R. Deng, J. Chen, X. Cao, Y. Zhang, S. Maharjan, and S. Gjessing, "Sensing-performance tradeoff in cognitive radio enabled smart grid," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 302–310, Mar. 2013.*
15. *R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.*
16. *S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar et al., "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," IEEE Access, vol. 5, pp. 25808–25825, 2017.*
17. *Siti Dhalila Mohd Satar, Mohamad Afendee Mohamed, Masnida Hussin, Zurina Mohd Hanapi and Siti Dhalila Mohd Satar, Cloud based Secure Healthcare Framework by using Enhanced Ciphertext Policy Attribute-Based Encryption Scheme International Journal of Advanced Computer Science and Applications (IJACSA), (2021) 12(6).*
18. *S. Srivastava and R. Kumar, "Indirect method to measure software quality using CK-OO suite," 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013, pp. 47-51, doi: 10.1109/ISSP.2013.6526872.*

19. *Ram Kumar, Gunja Varshney , Tourism Crisis Evaluation Using Fuzzy Artificial Neural network, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011*
20. *Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava, "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278– 4209*
21. *Kumar, R., Singh, J.P., Srivastava, G. (2014). Altered Fingerprint Identification and Classification Using SP Detection and Fuzzy Classification. In: , et al. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Advances in Intelligent Systems and Computing, vol 236. Springer, New Delhi. https://doi.org/10.1007/978-81-322-1602-5_139*
22. *Gite S.N, Dharmadhikari D.D, Ram Kumar," Educational Decision Making Based On GIS" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-1, April 2012.*
23. *Ram Kumar, Sarvesh Kumar, Kolte V. S.," A Model for Intrusion Detection Based on Undefined Distance", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1 Issue-5, November 2011*
24. *V. K. A. Sandor, Y. Lin, X. Li, F. Lin and S. Zhang, "Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage," Journal of Network and Computer Applications, vol. 129, pp. 25–36, 2019*
25. *X. Li, X. Liang, R. Lu, H. Zhu, X. Lin, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures and challenges," IEEE Common. Mag., vol. 58, no. 8, pp. 38–45, Aug. 2012.*
26. *Xu, R. and Lang, B., A CP-ABE Scheme with Hidden Policy and its Application in Cloud Computing. International Journal of Cloud Computing, 4(4) (2015) 279.*

******