Merkle Hash Tree with Hash based Digital Signature for Cloud Data Confidentiality and Security

AR.Arunachalam, G.Michael, R. Elankavi

Abstract*: It provides efficient processing power, an unbelievable computation speed and a wide array of stage space.Basically, the cloud computing transfer the huge volume of data on the different cloud servers which is maintained by the different kinds of cloud providers and this process help to remove the physical data's possession even though user are the data owners. This extraordinary element coordinates to raise the innumerable new security disadvantages which have not been surely known obviously. Consequently, in this paper present a novel methodology for secure cloud information stockpiling with the assistance of Merkle Hash Tree (MHT) with hash based advanced mark to give trustworthiness and protection of redistributed information in cloud using private key security approach. Additionally, in this work use theAdvanced Encryption Standard (AES) for conforming the data confidentiality and data security before the data is stored into the cloud. The simulation results show the better results in term of Data Recovery Time, Processing time, and efficiency respectively.

Keywords*: cloud data security, Merkle Hash Tree, hash based digital signatureAdvanced Encryption Standard (AES)

I. INTRODUCTION

Distributed computing is known as idea of the web based philosophy, which gives a various types of remote administrations through the web, for example, equipment, programming, information stockpiling, foundation, etc, which means utilizing a wide arrangement of controls, innovations, approaches and controls to applications, secure information and moreover connected with distributed computing framework [1]. The basic guidelines of the distributed computing procedure is establishing a compensation as you go business framework for data and registering innovation benefits that you will use, flexible augmenting scaling, on interest figuring administrations and end of operational costs and direct front capital [2]. In any case, in distributed computing the security assumes the most huge job and it has principle worry over the web in order to serve every one of the advantages and administrations of it.

Revised Manuscript Received on July 22, 2019.

Dr.AR.Arunachalam, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai , India. Email: ararunachalam78@gmail.com

G.Michael, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai , India. Email: micgeo270479@gmail.com

R. Elankavi, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai , India. Email: vimalamuthu3@gmail.com

Here, the information mystery over the system can be accomplished by using a portion of the cryptography technique which is the procedure of sort of hash capacity and encryption activity.

A cloud storage system is defined as a huge-scale ubiquitous storage system where countless storage servers are works and resided individually. In cloud each and every storage systems must have a property of robustness [3]. Countless methods or systems are implemented and presented for cloud data storage system. Normally the robustness is attained by utilizing conforming coding where the transferring message is segmented into k symbols of n code words. Each and every data is stored in the different storage symbol. So as to calculate the segmented data in a distributed cloud environment, the process is performed in parallel way [4]. Once the data is stored in the different storage sever, the data are computed with the help of hash value.

Today there are countless approaches and techniques are proposed by different kinds of authors to ensure cloud client in term of availability, confidentiality, and integrity of data given by cloud service providers [5]. However the integrity is known as extension of confidentiality which means what kinds of information is available in cloud, what is typically there, and is correctly protected against intentional or accidental alteration without authorization. Similarly the confidentiality defined as keep the information from the out of hands. At the same time legal protection, confidentiality is also supported by different kinds of technical tool for example encryption and access control. Availability is defined as the being able to utilize the cloud system as predictable by cloud users. In previous work the proxy re-encryption method is consider for data encryption is the data are encrypted with encoding operation and this process the data are stored in the receiver or client storage. However, the proxy re-encryption processes some drawback for example the data encryption process take long time which causes the time consuming process[8],[10],[12].

Thus, in this paperproposes a novel approach for secure cloud data storage with the help of Merkle Hash Tree (MHT) with hash based digital signature to provide integrity and privacy of outsourced data in cloud utilizing private key security approach. Additionally, in this work use the Advanced Encryption Standard (AES) for conforming the data confidentiality and data security before the data is stored into the cloud.

II. RELATED WORKS

[6] creator acquaints how with improve the Cloud stockpiling

security utilizing the execution of a hash functionsand half and half encryption calculation.

In this proposed work the executes two distinctive sort of calculations such asAdvanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) with a protected hashing calculation (SHA256) by using Netbeans IDE 8.0.2, EyeOS2.5 and JDK 1.7 instrument as a cloud stage on ubuntu14.04.

In [7] creator present edge intermediary re-encryption plan and which is coordinate with Fully Homomorphic Encryption is known as promising methodology for scrambled information' get to control.Here, the intermediary re-encryption plan used to processencodes and encoded messages from the information proprietor and it moreover advances to the capacity or receiverserver. The general execution accomplishes the designation progression with verified access control. The experimental results presents that the proposed system attains both backward security and forward security in cloud environment.

In [8] author present cloud storage system, while farm out trust worthiness of the data. To ensure the dynamic data storage integrity of cloud data, external Third Party Auditor (TPA) is used in a cloud infrastructure. For qualifying public auditing in cloud data storage security, users can alternative to an external auditor to checkof an outsourced data's integrity. The TPA should met the following essential necessities: 1) TPA should be able to proficiently audit the cloud data without illuminating the original data,2) Auditing process should not take no new susceptibilitiesat the time of auditing process, 3) data integrity is protected against TPA by raisingcertaincryptographic methods to guarantee the storage correctness in cloud[13],[15],[17]

In [9] author proposes a secure and efficient and protocol to address the secure data storage issue. In this work done based on Sobol Sequence (random sampling) and Elliptic Curve Cryptography.This work Permits TPA to intermittently check the data integrity stored at CSP without rescuing original data. In this work creates probabilistic proofs of cloud data integrity by perplexin grandom sets of blocks from the server, which radically minimize the communication and I/O costs. The challenge-constant amount of data, response protocol transmits, a small, which reduces network communication. Firstly, this protocol is very confidential: it never shows inside data to the malicious parties. This proposed work additionally considers the dynamic data operations at block level while upholding the same security declaration. This work eliminates the burden of user verification process from users, improves both the storage service's and user's fear about data corruptions and data leakage. Over security analysis, in this prove that proposed scheme is more efficient and secure[14],[16],[18]

In [10] author propose an enhanced technique which is consists of five donations such as Efficient third-party auditing service, image steganography, metadata generation, Partial homomorphic cryptography andresilient role-based access control mechanism, The main advantage in this work is to minimize time consumption on inspection files utilizing trusted TPA.

III. MERKLE HASH TREE (MHT)

The AMHT is one of the well-known authentication structures and basically the MHT is utilized to effectively prove that a set of elements are unaltered and undamaged. It greatly uses for reduces the server processing time. Advanced Encryption Standard (AES) is used for authenticating process. In MHT the leaf node have has values, the main idea behind this process is break the file into different number of blocks. The hash value is known as authentic data value which means the original files blocks and these blocks are iteratively combining when data blocks are subtracted. Now, the hash values are rehash the outcome nodes and which nodes are combine in a tree-like repeat and fashion this process till process when get a tree with a single root. This process created by the cloud client and is stored at both server side and cline side[31],[33],[35]. Figure 1 shows that the typical MHT which has four leaf nodes such as . Initially, employ the hash on each and every data blocks and which extract , after this process are combined and again hashed together to get . Parallel process may happens with node , finally here get , where h is defined as hash function.

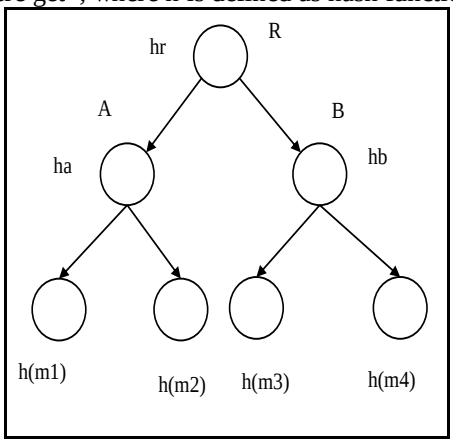


Figure 1- Merkle Hash Tree (MHT)

This can be stated as

$$ha = h(h(m1)||h(m2)) \; and \; hb = h(h(m3)||h(m4)) \quad (1)$$

Further, $ha \; and \; hb$ are rehashed and combined to obtain the root as hr which is defined as

$$hr = h(ha||hb) \quad (2)$$

Notations

F- defined as File stored at the untrusted server

E_{sk} defined as Encryption using Secret key

T defined as Tag (signature)

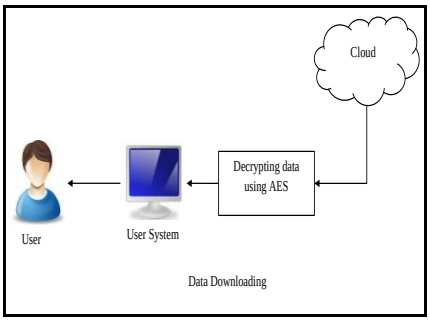
m is defined as File block

$\Phi$is defined as Set of tags

Initially, the data $D = \{m1, m2 \ldots mn\}$ is produced by the client, which is a finite gathering on n node.

Utilizing the key generation procedure, here the secret key is generated..

After this process a signature is created for each and every data block utilizing the SHA1 hash and secret key algorithm. This is done as $T_i = Esk(H(m_i))$, where m_i is the ith block of the file. After this process, a set ofsignatures of file blocks $\Phi = \{T_i\}$ is produced, also known as the set of Tags. Then MHT is assembled and then, the root of the tree is contracted utilizing the secret key as $sigsk\ (H(R))$. Finally, the client publicizes$\{F, \Phi, sigsk(H(R))\}$ to the server and deletes F and $sigsk(H(R))$ from its local storage. Additionally, in this work use the Advanced Encryption Standard (AES) for conforming the data confidentiality and data security before the data is stored into the cloud is shown in Figure 2 (a) and (b) in term of data uploading and data downloading process.



Here assume that peer node in cluster , define by access the node probability . A MHT based access is considered by following rules[32],[34],[36]

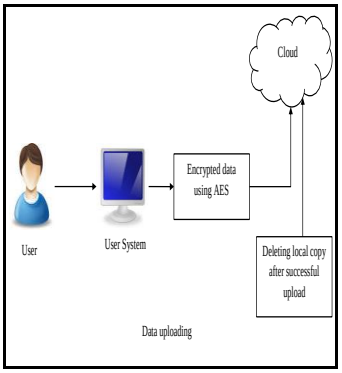
Step1 : is utilized to defined a set that has trees (only one root node in each and every tree);

Step 2: Three trees with highest access probability are elected to create a new tree. Depends on the probability's descending order, they are as the new tree's right sub-tree, middle sub-treeand left sub-tree(when two root nodes with numbers of tree, equal access probability are concerns), and new tree access probability is the sum of old trees.

Step 3: Remove those above mentioned trees from the set $F = p_1, p_2, \ldots, p_n$, moreover, put the new tree in the set.

Step 4: Step 2 and 3 are reprocess until there is only one tree in set $F = p_1, p_2, \ldots, p_n$, the last tree is result that here want[38],[40]

Step 5: The definition of MHT defined that the no of leaf nodes in a MHT must fulfills condition $num = 2t + 1$, hence, when do not fulfills that condition, here can add a virtual node with kind of access probability 0 in set $F = p_1, p_2, \ldots, p_n$ so as to build MHT.



IV. RESULTS AND DISCUSSIONS

Figure 3 shows that the total processing time which is compared with Secure Hash Algorithm (SHA256),Scalable Provable Data Possession(S-PDP) and proposed Merkle Hash Tree (MHT) with Advanced Encryption Standard (AES). From the results the proposed MHT+AES shows that the minimum processing time when compared with other three methods such as proxy re-encryption, SHA256 and S-PDP.

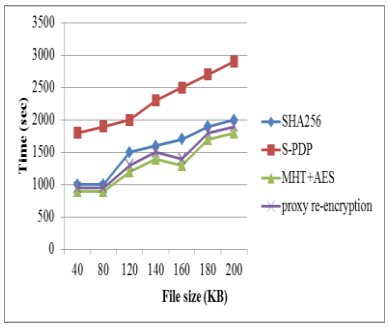


Figure 2 - Processing time

Figure 2 shows that the Data Recovery Time which is compared with Secure Hash Algorithm (SHA256),Scalable Provable Data Possession(SPDP) and proposed Merkle Hash Tree (MHT) with Advanced Encryption Standard (AES). From the results the proposed MHT+AES shows that the minimum Data Recovery Timewhen compared with other three methods such as proxy re-encryption, SHA256 and S-PDP[37],[39],[41].

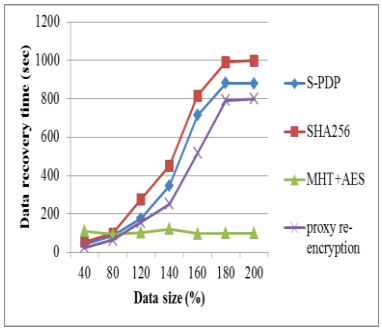


Figure 3 - Data Recovery Time

V. CONCLUSION

The The This paper present a novel approach for secure cloud data storage with the help of MHT with hash based digital signature to provideand privacy integrityof outsourced data in cloud utilizing private key security approach.However, the previous proxy re-encryption processes has some drawback for example the data encryption process take long time which causes the time consuming process. Thus, in this work proposes a new method as MHT with hash based digital signature with AES procedure. The simulation results show the better results in term of Data Recovery Time, Processing time, and efficiency respectively.Moreover, for security process use AES for conforming the data confidentiality and data security before the data is stored into the cloud.

REFERENCES

[1] Kumaravel A., Rangarajan K.,Algorithm for automaton specification for exploring dynamic labyrinths,Indian Journal of Science and Technology,V-6,I-SUPPL5,PP-4554-4559,Y-2013

[2] P. Kavitha, S. Prabakaran "A Novel Hybrid Segmentation Method with Particle Swarm Optimization and Fuzzy C-Mean Based On Partitioning the Image for Detecting Lung Cancer" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019

[3] Kumaravel A., Meetei O.N.,An application of non-uniform cellular automata for efficient cryptography,2013 IEEE Conference on Information and Communication Technologies, ICT 2013,V-,I-,PP-1200-1205,Y-2013

[4] Kumarave A., Rangarajan K.,Routing alogrithm over semi-regular tessellations,2013 IEEE Conference on Information and Communication Technologies, ICT 2013,V-,I-,PP-1180-1184,Y-2013

[5] P. Kavitha, S. Prabakaran "Designing a Feature Vector for Statistical Texture Analysis of Brain Tumor" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019

[6] Dutta P., Kumaravel A.,A novel approach to trust based identification of leaders in social networks,Indian Journal of Science and Technology,V-9,I-10,PP--,Y-2016

[7] Kumaravel A., Dutta P.,Application of Pca for context selection for collaborative filtering,Middle - East Journal of Scientific Research,V-20,I-1,PP-88-93,Y-2014

[8] Kumaravel A., Rangarajan K.,Constructing an automaton for exploring dynamic labyrinths,2012 International Conference on Radar, Communication and Computing, ICRCC 2012,V-,I-,PP-161-165,Y-2012

[9] P. Kavitha, S. Prabakaran "Adaptive Bilateral Filter for Multi-Resolution in Brain Tumor Recognition" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019

[10] Kumaravel A.,Comparison of two multi-classification approaches for detecting network attacks,World Applied Sciences Journal,V-27,I-11,PP-1461-1465,Y-2013

[11] Tariq J., Kumaravel A.,Construction of cellular automata over hexagonal and triangular tessellations for path planning of multi-robots,2016 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2016,V-,I-,PP--,Y-2017

[12] Sudha M., Kumaravel A.,Analysis and measurement of wave guides using poisson method,Indonesian Journal of Electrical Engineering and Computer Science,V-8,I-2,PP-546-548,Y-2017

[13] Ayyappan G., Nalini C., Kumaravel A.,Various approaches of knowledge transfer in academic social network,International Journal of Engineering and Technology,V-,I-,PP-2791-2794,Y-2017

[14] Kaliyamurthie, K.P., Sivaraman, K., Ramesh, S. Imposing patient data privacy in wireless medical sensor networks through homomorphic cryptosystems 2016, Journal of Chemical and Pharmaceutical Sciences92.

[15] Kaliyamurthie, K.P., Balasubramanian, P.C. An approach to multi secure to historical malformed documents using integer ripple transfiguration 2016 Journal of Chemical and Pharmaceutical Sciences92.

[16] A.Sangeetha,C.Nalini,"Semantic Ranking based on keywords extractions in the web", International Journal of Engineering & Technology, 7 (2.6) (2018) 290-292

[17] S.V.GayathiriDevi,C.Nalini,N.Kumar,"An efficient software verification using multi-layered software verification tool "International Journal of Engineering & Technology, 7(2.21)2018 454-457

[18] C.Nalini,ShwtambariKharabe,"A Comparative Study On Different Techniques Used For Finger – Vein Authentication", International Journal Of Pure And Applied Mathematics, Volume 116 No. 8 2017, 327-333, Issn: 1314-3395

[19] M.S. Vivekanandan and Dr. C. Rajabhushanam, "Enabling Privacy Protection and Content Assurance in Geo-Social Networks", International Journal of Innovative Research in Management, Engineering and Technology, Vol 3, Issue 4, pp. 49-55, April 2018.

[20] Dr. C. Rajabhushanam, V. Karthik, and G. Vivek, "Elasticity in Cloud Computing", International Journal of Innovative Research in Management, Engineering and Technology, Vol 3, Issue 4, pp. 104-111, April 2018.

[21] K. Rangaswamy and Dr. C. Rajabhushanamc, "CCN-Based Congestion Control Mechanism In Dynamic Networks", International Journal of Innovative Research in Management, Engineering and Technology, Vol 3, Issue 4, pp. 117-119, April 2018.

[22] Kavitha, R., Nedunchelian, R., "Domain-specific Search engine optimization using healthcare ontology and a neural network backpropagation approach", 2017, Research Journal of Biotechnology, Special Issue 2:157-166

[23] Kavitha, G., Kavitha, R., "An analysis to improve throughput of high-power hubs in mobile ad hoc network" , 2016, Journal of Chemical and Pharmaceutical Sciences, Vol-9, Issue-2: 361-363

[24] Kavitha, G., Kavitha, R., "Dipping interference to supplement throughput in MANET" , 2016, Journal of Chemical and Pharmaceutical Sciences, Vol-9, Issue-2: 357-360

[25] Michael, G., Chandrasekar, A.,"Leader election based malicious detection and response system in MANET using mechanism design approach", Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .

[26] Michael, G., Chandrasekar, A.,"Modeling of detection of camouflaging worm using epidemic dynamic model and power spectral density", Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .

[27] Pothumani, S., Sriram, M., Sridhar, J., Arul Selvan, G., Secure mobile agents communication on intranet,Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg No S32-S35, 2016

[28] Pothumani, S., Sriram, M., Sridhar , Various schemes for database encryption-a survey, Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg NoS103-S106, 2016

[29] Pothumani, S., Sriram, M., Sridhar, A novel economic framework for cloud and grid computing, Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg No S29-S31, 2016

[30] Priya, N., Sridhar, J., Sriram, M. "Ecommerce Transaction Security Challenges and Prevention Methods- New Approach" 2016 ,Journal of Chemical and Pharmaceutical Sciences, JCPS Volume 9 Issue 3.page no:S66-S68 .

[31] Priya, N.,Sridhar,J.,Sriram, M."Vehicular cloud computing security issues and solutions" Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016

[32] Priya, N., Sridhar, J., Sriram, M. "Mobile large data storage security in cloud computing environment-a new approach" JCPS Volume 9 Issue 2. April - June 2016

[33] Anuradha.C, Khanna.V, "Improving network performance and security in WSN using decentralized hypothesis testing "Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .

[34] Anuradha.C, Khanna.V, "A novel gsm based control for e-devices" Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .

[35] Anuradha.C, Khanna.V, "Secured privacy preserving sharing and data integration in mobile web environments " Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .

[36] Sundarraj, B., Kaliyamurthie, K.P. Social network analysis for decisive the ultimate classification from the ensemble to boost accuracy rates 2016 International Journal of Pharmacy and Technology

[37] Sundarraj, B., Kaliyamurthie, K.P. A content-based spam filtering approach victimisation artificial neural networks 2016 International Journal of Pharmacy and Technology83.

[38] Sundarraj, B., Kaliyamurthie, K.P. Remote sensing imaging for satellite image segmentation 2016 International Journal of Pharmacy and Technology8 3.

[39] Sivaraman, K., Senthil, M. Intuitive driver proxy control using artificial intelligence 2016 International Journal of Pharmacy and Technology84.

[40] Sivaraman, K., Kaliyamurthie, K.P. Cloud computing in mobile technology 2016 Journal of Chemical and Pharmaceutical Sciences92.

[41] Sivaraman, K., Khanna, V. Implementation of an extension for browser to detect vulnerable elements on web pages and avoid click jacking 2016 Journal of Chemical and Pharmaceutical Sciences92.

AUTHORS PROFILE

Dr.AR.Arunachalam Associate Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

G.Michael Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

R. Elankavi Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India