ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Database Security with Access Control and Assured Deletion Using Cryptographic Key

S.Sumathi[1], K.G.S.Venkatesan[2], R.Karthikeyan [3]

Dept. of C.S.E., Bharath University (BIHER), Chennai, Tamil Nadu, India

Associate Professor, Dept. of C.S.E., Bharath University (BIHER), Chennai, Tamil Nadu, India

Associate Professor, Dept. of C.S.E., Bharath University (BIHER), Chennai, Tamil Nadu, India

ABSTRACT: The outsource information reinforcements off-site to outsider distributed storage benefits in order to decrease information administration costs. Be that as it may, the maker of cloud must give security sureties to the outsourced information, which is presently kept up by outsiders. To plan and execute FADE, a safe overlay distributed storage framework that accomplishes fine-grained, arrangement based access control and document guaranteed cancellation. It partners outsourced records with document access arrangements, and without a doubt erases documents to make them unrecoverable to heaps of document access approaches. To accomplish such security objectives, FADE is based upon an arrangement of cryptographic key operations that are self-kept up by a majority of key administrators that are autonomous of outsider mists. Specifically, FADE goes about as an overlay framework that works consistently a top today's distributed storage administrations and actualize a proof-of-idea model of FADE on Amazon S3, one of today's distributed storage administrations. To direct broad observational studies, and show that FADE gives security insurance to outsourced information, while presenting just negligible execution and money related cost overhead. Our work gives experiences of how to join esteem included security highlights into today's distributed storage administrations.

KEYWORDS: Cryptographic key, Key Manager, Cloud Storage, Data source

I. Introduction

Distributed storage is another business answer for remote reinforcement outsourcing, as it offers a deliberation of limitless storage room for customers to host information reinforcements in a pay-as you - go way. It helps endeavors and government organizations altogether lessen their budgetary overhead of information administration, since they can now document their information reinforcements remotely to outsider distributed storage suppliers as opposed to keep up server farms all alone. For instance, Smug Mug, a photograph sharing site, facilitated terabytes of photographs on Amazon S3 in 2008 and spared a large number of dollars on keeping up capacity gadgets. More contextual investigations of utilizing distributed storage for remote reinforcement can be found in. Aside from undertakings and government offices, people can likewise document their own information to the cloud utilizing apparatuses like Drop box. Specifically, with the approach of Smartphone, desire is that more individuals will utilize Drop box - like apparatuses to move sound/video documents from their Smartphone to the cloud, given that Smartphone normally have constrained capacity assets. Be that as it may, security concerns get to be important as to now outsource the capacity of potentially delicate information to outsiders.

In this paper, the makers are especially intrigued by two security issues. To begin with, the engineer need to give sureties of access control, in which to guarantee that just approved gatherings can get to the outsourced information on the cloud. Specifically, designer must restrict outsider distributed storage suppliers from mining any touchy data of their customers' information for their own showcasing purposes. Second, it is vital to give insurances of guaranteed erasure, implying that outsourced information is for all time out of reach to anyone (counting the information) heaps of cancellation of information. Keeping information for all time is undesirable, as information might be startlingly uncovered later on because of noxious assaults on the cloud or rushed administration of cloud administrators.

DOI: 10.15680/IJIRCCE.2016. 0403198

II. LITERATURE SURVEY

- **TRANSACTIONS AND DEPENDABABLE AND SECURE COMPUTING**

The reason for TDSC is to distribute papers in reliability and security, including the joint thought of these issues and their interchange with framework execution. These zones incorporate however are not constrained to: System Design: engineering for secure and blame tolerant frameworks, trusted/survivable processing, interruption and mistake resistance, recognition and recuperation, flaw and interruption tolerant middleware, firewall and system advances, framework administration and organization. Assessment: demonstrating and forecast, survivability and perform capacity displaying, arrangement procedures, trial strategies including test-bed outline, computerized deficiency/assault era, observing, estimation and examination, workload portrayal, benchmarking, and nature of administration evaluation.

Applications: exchange handling, appropriated and pervasive frameworks, electronic business, continuous frameworks, security basic frameworks, installed frameworks, Internet applications. Programming Design: working framework support for identification and recuperation, self checking, adaptation to internal failure procedures, system interfaces and conventions, testing, acceptance, confirmation, maturing and revival, unwavering quality and execution. Developing Technologies: nanoscale figuring, portable registering, remote telephony, satellite systems, information mining, wearable PCs, media applications, signal preparing, quantum processing.

- **PRIVACY-PRESERVING PUBLIC AUDITING FOR STORAGE SECURITY**

Distributed computing Distributed computing is the since quite a while ago envisioned vision of figuring as an utility, where clients can remotely store their information into the cloud to appreciate the on-interest fantastic applications and administrations from a common pool of configuraurable registering assets. By information outsourcing, clients can be calmed from the weight of nearby information stockpiling and support. In any case, the way that clients no more have physical ownership of the perhaps huge size of outsourced information makes the information respectability security in Cloud Computing an exceptionally difficult and possibly considerable undertaking, particularly for clients with obliged figuring assets and abilities.

- **CIPHER TEXT-POLICY ATTRIBUTE BASED ENCRYPTION**

The idea of characteristic based encryption was initially proposed in a point of interest work by Amit Sahai and Brent Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters. It is a kind of open key encryption in which the mystery key of a client and the content are indigent upon characteristics (e.g. the nation he lives, or the sort of membership he has). In such a framework, the decoding of a content is conceivable just if the arrangement of traits of the client key matches the qualities of the figure content

III. EXISTING SYSTEM

The keys which we are utilized as a part of this are in scrambled structure and it was put away in the cloud database. Despite the fact that the keys are in encoded structure the programmers might utilize some exceptional system to decode the keys and get to the information. In such cases the programmers might change the information or lost the information. Because of this security level will be diminished, and it will give less proficiency. By utilizing the key era calculation which does not make the productive process and makes cheatable cloud calculation and security can't be accomplished. It additionally lost the information stockpiling security and calculation inspecting security and in addition protection deceiving disheartening. Augments the calculation cost because of advancement issue.

IV. PROPOSED SYSTEM

To defeat the issue of existing framework, proposed a unique mark confirmation plan utilizing the idea of Merkle Hash Tree. The information proprietor stores the document in an encoded structure in the cloud server. The cloud client needs to enlist with the proprietor alongside the root signature. The Fingerprint format is part it into eight shares utilizing picture handling system as a part of the customer side. The splitted eight shares are given as inputs to merkle hash tree where in every offer needs to experience hashing capacity and consequently root mark is produced. The mark is created and put away in the Jelastic cloud server (Jelastic cloud is an open cloud which is utilized to get to the record put away in the jelastic cloud database with legitimate mail id and password).The client needs to present the adjoining and kin shares of unique mark layout for confirmation reason. The mark is created in the cloud administration supplier and in this way confirmed with the put away mark in the cloud. The abuse of delicate information can be stayed away from and this gives a viable and proficient client remote confirmation with the cloud.

Advantages of Proposed System

- The abuse of touchy information is stayed away from.
- It gives a successful and productive client remote confirmation with the cloud.
- Fingerprint confirmation
- It gives Assured cancellation utilizing Cryptographic key.

V. SECURE OVERLAY CLOUD STORAGE

The information proprietor stores the document in an encoded structure in the cloud server. The cloud client needs to enlist with the proprietor alongside the root signature. The Fingerprint format is part it into eight shares utilizing picture preparing method as a part of the customer side. The splitted eight shares are given as inputs to merkle hash tree where in every offer needs to experience hashing capacity and henceforth root mark is produced. The mark is created and put away in the Jelastic cloud server (Jelastic cloud is an open cloud which is utilized to get to the document put away in the Jelastic cloud database with substantial mail id and password).The client needs to present the contiguous and kin shares of unique finger impression format for confirmation reason. The mark is created in the cloud administration supplier and along these lines confirmed with the put away mark in the cloud. The abuse of delicate information can be dodged and this gives a viable and proficient client remote confirmation with the cloud.

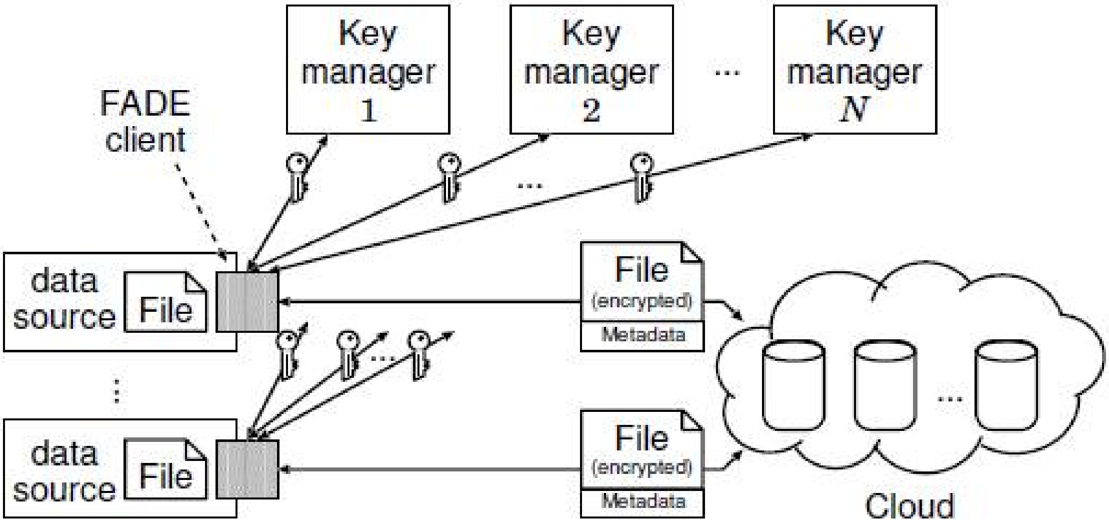

Figure1: Block Diagram of cloud storage

5.1 CRYPTOGRAPHIC KEYS

JELASTIC characterizes three sorts of cryptographic keys to secure information documents put away on the cloud.

5.1.1 DATA KEY

An information key is an arbitrary mystery that is created and kept up by a JELASTIC customer. It is utilized for encoding or decoding information records by means of symmetric-key encryption (e.g., AES).

5.1.2 CONTROL KEY

A control key is connected with a specific strategy. It is spoken to by an open private key pair, and the private control key is kept up by the majority of key chiefs. It is utilized to scramble/unscramble the information keys of the documents ensured with the same approach. The control key structures the premise of approach based guaranteed cancellation.

5.1.3 ACCESS KEY

Like the control key, an entrance key is connected with a specific arrangement, and is spoken to by an open private key pair. In any case, dissimilar to the control key, the private access key is kept up by a JELASTIC customer that is approved to get to records of the related arrangement. The entrance key is based on property based encryption, and structures the premise of strategy based access control. Naturally, to effectively decode a scrambled document put away on the cloud, To require the right information key, control key, and get to key. With no of these keys, it is computationally infeasible to recoup an outsourced document being secured by JELASTIC. The accompanying discloses how to oversee such keys to accomplish our security objectives.

5.2 JELASTIC OVERVIEW

The configuration of JELASTIC, a framework that gives sureties of access control and guaranteed cancellation for outsourced information in distributed storage. To display the fundamental segments of JELASTIC, and state the configuration and security objectives that it tries to accomplish. The cloud has information documents for the benefit of a gathering of JELASTIC clients who need to outsource information records to the cloud in view of their meanings of document access strategies. JELASTIC can be seen as an overlay framework on the basic cloud. It applies security assurance to the outsourced information documents before they are facilitated on the cloud.

5.2.1 KEY MANAGERS

JELASTIC is based on a majority of key administrators, each of which is a stand-alone substance that keeps up strategy based keys for access control and guaranteed cancellation, the cloud kept up by an outsider supplier, gives storage room to facilitating information documents in the interest of various JELASTIC customers in a pay-as-you-go way. Each of the information documents is connected with a mix of record access arrangements. JELASTIC is based on the manager cloud interface, and accept just the essential cloud operations for transferring and downloading information documents. To underscore that to don't require any convention and usage changes on the cloud to bolster JELASTIC.

5.2.2 POLICY-BASED ACCESS CONTROL

A JELASTIC customer is approved to get to just the documents whose related arrangements are dynamic and are fulfilled by the customer.

5.2.3 POLICY-BASED ASSURED DELETION

A document is erased (or for all time out of reach) if its related approaches are denied and get to be out of date. That is, regardless of the possibility that a document duplicate that is connected with denied strategies exists, it remains scrambled and to can't recover the comparing cryptographic keys to recuperate the record. In this way, the document duplicate gets to be unrecoverable by anybody (counting the proprietor of the record).

5.3 JELASTIC SERVER MODULE

Jelastic group has made a module for Netbeans advancement stage that streamlines the procedure of use administration and improvement in jelastic stage. Before access the jelastic cloud, the client gives the suitable mail id and secret word to login into the Jelastic cloud. After that client introduce the jelastic plug in into the netbeans. The client need to get to the Jelastic cloud implies, client must give the same mail id and secret key which the client give for Jelastic cloud enrollment. On the off chance that the given mail id and secret key is right then the client can get to the information or else can't get to the information.

5.3.1 GENERATE ROOT SIGNATURE

In this module, clarifies the proprietor's part in jelastic server. The proprietor check the client's mail id, secret word and unique mark. On the off chance that the given points of interest are coordinated for the put away one, then the proprietor split the unique mark picture into eight sections utilizing limit part calculation. And afterward the splitted eight sections are given as data to the merkle hash tree and make pull signature for the given unique mark picture. At that point the proprietor gives the root mark to the Jelastic server and it was put away in the Jelastic server.

5.3.2 SEND ROOT SIGNATURE

Root mark will spare encoded position in jelastic server utilizing Advanced Encryption Standard. In the client name, secret word and attach mark will send to the enrolled mail id utilizing Simple Mail Transfer Protocol (SMTP).If the client's given root mark are coordinated to the database root signature then the client can get to the server.

5.3.3 SHARE FILE

In this module the undertaking administrator can transfer the record and necessities to the jelastic cloud for supplier designation. In this we utilize AES(Advanced Encryption Standard) calculation to scramble the record. The encoded records are spared into the Jelastic cloud database. By utilizing the Symmetric key Encryption technique the undertaking administrator might make the protected key and send to the client.

5.3.4 ACCESS FILE

The task supervisor will send the way to the client. At whatever point the client need to get to the record put away in the Jelastic cloud, the client must enter the substantial key. On the off chance that the client need to get to or unscramble the document then he/she should enter the Secure key.

5.3.5 FILE SUSTAINABILITY

After get the administration to get to the record, the client must get to the document inside of specific days. In the event that the client doesn't access the document specifically days, then it got terminated. Once the document will be lapsed then the client can't ready to get to the record. At that point the client offers solicitation to the proprietor to broaden the legitimacy time of the document. In the event that the proprietor acknowledges the solicitation then the client can get to the record.

5.4 FILE UPLOAD/DOWNLOAD

To now present the essential operations of how a customer transfers/downloads records to/from the cloud. To begin with the situation where every record is connected with a solitary approach, and afterward clarifies how a document is connected with various strategies. Our outline depends on blinded RSA (or blinded decoding), in which the customer demands the key chief to unscramble a blinded adaptation of the encoded information key. On the off chance that the related arrangement is fulfilled, then the key administrator will unscramble and give back the blinded variant of the first information key. The customer can then recoup the information key. The inspiration of utilizing this

DOI: 10.15680/IJIRCCE.2016. 0403198

blinded decoding methodology is that the real substance of the information key stays secret to the key chief as Toll as to any assailant that sniffs the correspondence between the customer and the key director.

5.4.1 FILE UPLOAD

In Figure 2,the customer first demands the general population control key (ni, ei) of arrangement Pi from the key supervisor, and reserves (ni, ei) for resulting utilizes if the same strategy Pi is connected with different documents.

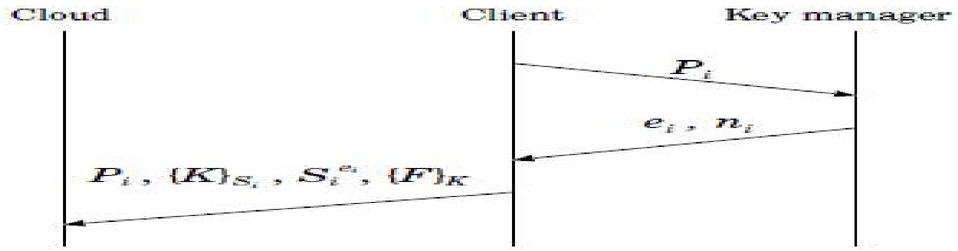

Figure 2 : File Upload Operation

Then the client generates two random keys K and Si, and sends {K}Si , Sei i , and {F}K to the cloud2. Then the client must discard K and Si. To protect the integrity of a file, the client computes an HMAC signature on every encrypted file and stores the HMAC signature together with the encrypted file in the cloud. Assume that the client has a long-term private secret value for the HMAC computation.

5.4.2 FILE DOWNLOAD

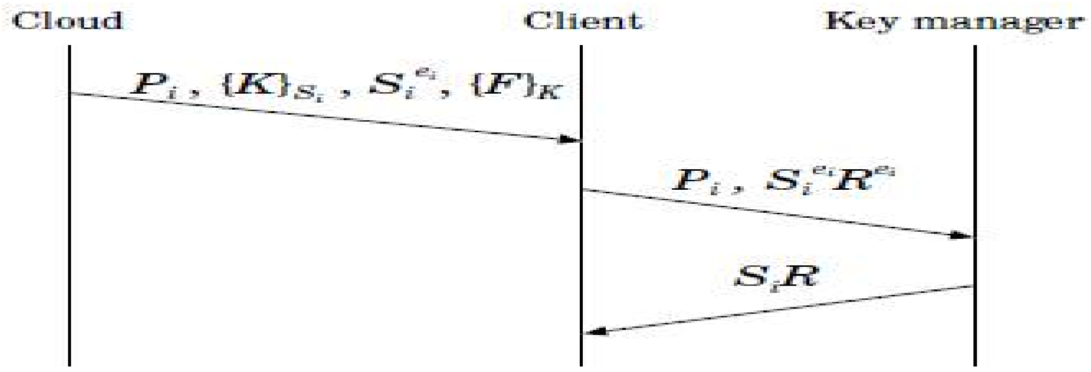
Cloud
Client
Key manager
P_i , $\{K\}_{S_i}$, $S_i^{e_i}$, $\{F\}_K$
P_i , $S_i^{e_i}R^{e_i}$
S_iR

Figure 3: File Download Operation

At that point the customer creates two irregular keys K and Si, and sends {K}Si , Sei i , and {F}K to the cloud2. At that point the customer must toss K and Si. To secure the respectability of a record, the customer Figures a HMAC signature on each encoded document and stores the HMAC signature together with the scrambled document in the cloud. Expect that the customer has a long haul private mystery esteem for the HMAC calculation the customer brings {K}Si , Sei i , and {F}K from the cloud. The customer will first check whether the HMAC mark is substantial before unscrambling the document. At that point the customer produces a mystery irregular number R, Rei , and sends Sei i •Rei = (SiR)ei to the key administrator to ask for decoding. The key director then processes and returns ((SiR)ei)di = SiR to the customer, which can now evacuate R and get Si, and decode {K}Si and thus {F}K.

5.5 SECURITY ANALYSIS

JELASTIC is intended to shield outsourced information from unapproved access and to certainly erase outsourced information. To now quickly abridge how JELASTIC accomplishes its security properties as depicted. In our setting, the distributed storage is endowed and unstable. The cloud might at present keep reinforcement duplicates of any outsourced record after it is asked for cancellation. Assume that an assailant accesses the distributed storage and gets the (scrambled) duplicates of all dynamic and erased records. Presently To contend that the assailant can't recuperate any information from those records ensured with JELASTIC.

5.5.1 ACTIVE FILES

A dynamic record on the cloud is encoded with an information key, which must be unscrambled by the key chief. So as to uncover the first information, the aggressor needs to ask for the key director to decode the information key. As talked about, the reaction from the key director is secured with the ABE-based access key. For whatever length of time that the aggressor does not have the entrance key, it can't decode the information key, and henceforth can't unscramble the first information.

5.5.2 DELETED FILES

A document gets to be erased when its related approach is disavowed. An erased record is still scrambled with an information key. Be that as it may, following the key supervisor has cleansed the control key for the renounced arrangement for all time, it loses the capacity to unscramble the information key. Consequently, the aggressor can't recoup the first information. In addition, regardless of the fact that the assailant is sufficiently intense to get the ABE access key or bargain the key chief to get all control keys, the first information of the erased record is still unrecoverable as the comparing control key is as of now arranged.

5.6 CLIENT

Our customer usage utilizes four capacity calls to empower end clients to collaborate with the cloud.

5.6.1 UPLOAD

The customer encodes the data document as indicated by the predefined arrangement (or a Boolean mix of approaches). Here, the document is scrambled utilizing the 128-piece AES calculation with the square binding (CBC) mode. After encryption, the customer additionally annexes the scrambled document size (8 bytes in length) and the HMAC-SHA1 signature (25 bytes in length) to the end of encoded record for trustworthiness checking in later downloads. It then sends the encoded document and the metadata.

5.6.2 DOWNLOAD

The customer recovers the record and strategy metadata from the cloud. It then checks the respectability of the encoded record, and unscrambles the document.

5.7 SPACE UTILIZATION OF CLOUD ARCHITECTURE

Presently get to the space usage. As expressed, every information record is went with its document size (10 bytes), the HMAC-SHA1 signature (25 byte), and metadata record that stores the strategy data and cryptographic keys. For the metadata document, its size contrasts with the quantity of arrangements and the quantity of key administrators utilized. Here, to break down the space overhead because of the metadata presented by JELA. The diverse sizes of the metadata in view of our execution model for a variable number of (a) conjunctive arrangements (P1 ^ P2 ^ • •^Pm), and (b) disjunctive strategies (P1 _P2 _• • •_Pm). To see how every metadata size is gotten, to consider the least difficult situation where there is just a solitary strategy and a solitary key director. At that point to need: (i) 128 bytes for every offer of the approach based mystery key Sei i for strategy i, (ii) 16 bytes for the scrambled duplicate of K in view of 128-piece AES, (iii) 4 bytes for the arrangement identifier, and (iv) 1 byte for the delimiter between the approach identifier and the keys. For this situation, the metadata size is 149 bytes. Note that on account of numerous approaches, to need to store more strategy identifiers as Toll as more cryptographic keys, and consequently the metadata size increments. Additionally, the metadata size increments with the quantity of key administrators. This space overhead turns out to be less noteworthy if the document size is sufficiently substantial (e.g., on the megabyte scale).

5.8 ESTIMATING COST MODEL

Assess the money related overhead of JELASTIC utilizing a basic estimating model. Here, to utilize a disentangled estimating plan of Amazon S3 in Thailand, in which To expect that our stockpiling utilization is under 2TB and our month to month information outbound exchange size is under 10TB. To gauge the expense of JELASTIC in light of Cumulus, a depiction based reinforcement framework. In, it is demonstrated that a run of the mill packed preview comprises of several fragments, each of which is around five megabytes. Here, to accept that our information source has s records (fragments) and every document is f bytes. Assume that every section is connected with p policies4, and there are N key administrators. To assess the expense when every record is transferred u times and downloaded d times. To signify by meta(p, N) the extent of the metadata, which is an element of p (number of strategies) and N (number of key chiefs).

To demonstrate the distinctive sizes of the metadata taking into account our execution, and demonstrates our improved evaluating plan (starting July 2012) and the comparing cost results. Represent, to connect to some case values as takes after. To let s = 310 and f = 5MB, for an aggregate of 2.5GB information. To utilize 3 conjunctive arrangements and 4 key directors. Expect that every document is transferred once and downloaded once and the additional expense that JELASTIC acquires is under 2.4% every month.

VI. CONCLUSION

Proposed a commonsense distributed storage framework called Jelastic, which give access control and guaranteed cancellation for documents that are facilitated by distributed storage administrations. To partner records with document access arrangements that control how records can be gotten to and after that present strategy based document guaranteed erasure, in which records are definitely erased and made unrecoverable by anybody when their related record access strategies are disavowed. The vital operations on cryptographic keys in order to accomplish access control and guaranteed erasure. The execution of model of Jelastic to show its common sense, and exactly contemplate its execution overhead when it works with Amazon S3. Our trial results give bits of knowledge into the execution security exchange off when JELASTIC is sent by and by. In this venture another methodology of remote client unique finger impression confirmation plan utilizing the idea of Merkle Hash Tree has been proposed.

The information proprietor stores the record in an encoded structure in the cloud server. The cloud client needs to enlist with the proprietor alongside the root signature. In the customer side, the Fingerprint format is part it into eight shares utilizing picture handling method. The splitted eight shares are given as inputs to merkle hash tree wherein every offer needs to experience hashing capacity and thus root mark is created. The mark is created and put away in the cloud server. The client needs to present the contiguous and kin shares of unique finger impression format for validation reason. The mark is created in the cloud administration supplier and in this manner checked with the put away mark in the cloud. The abuse of delicate information can be maintained a strategic distance from and this provide*s a successful and productive client remote validation with the cloud.

VII. ACKNOWLEDGEMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD of Computer Science & Engineering, **Dr. K.P. Kaliyamurthie,** Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank **Dr. A. Kumaravel, Dean** School of Computing, for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science &Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

1. C. Wang, Q. Wang, K. Ren, and W. Lou." Privacy-preserving public auditing for storage security in cloud computing". In Proc. of IEEE INFOCOM, Mar 2010.
2. H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon. RACS: "A Case for Cloud Storage Diversity". In Proc. of IEEE ACM SoCC, 2010.
3. J. Bethencourt, A. Sahai, and B. Waters. "Cipher text-Policy Attribute-Based Encryption". In Proc. of IEEE Symp. on Security and Privacy, May 2006.
4. Yang Tang, Patrick P. C. Lee, John C. S. Lui, Radia Perlman "Transactions And Dependable And Secure Computing" IEEE , VOL.9 NO.6, 2012
5. N. Dukkipati and N. McKeown. Why Flow-Completion Time is the Right Metric for Congestion Control. ACM SIGCOMM Computer Communication Review, 2006.
6. L. S. Brakmo, S. W. O'Malley, and L. L. Peterson. TCP Vegas: New Techniques for Congestion Detection and Avoidance. ACM SIGCOMM Computer Communication Review, 1994.
7. S. Ha, I. Rhee, and L. Xu. CUBIC: a New TCP-friendly High- Speed TCP Variant. ACM SIGOPS Operating System Review, 2008.
8. K. Tan, J. Song, Q. Zhang, and M. Sridharan. A Compound TCP Approach for High-Speed and Long Distance Networks. In Proc. IEEE INFOCOM, 2006.
9. L. Xu, K. Harfoush, and I. Rhee. Binary Increase Congestion Control (BIC) for Fast Long-Distance Networks. In INFOCOM 2004.
10. V. N. Padmanabhan and R. H. Katz. TCP Fast Start: A Technique for Speeding Up Web Transfers. In Proc. IEEE Global Internet Conference (GLOBECOM), 1998.
11. K. Winstein and H. Balakrishnan. TCP Ex Machina: Computer generated Congestion Control. In Proc. ACM SIGCOMM, 2013.
12. B. Sundarraj, K.G.S. Venkatesan, M. Sriram, Vimal Chand, "An Iaas cloud system with Federation Threshold", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2593 – 2598, March -2015.
13. K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.
14. S. Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network Infrastructures", International journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April - 2013.
15. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
16. P. Indira Priya, K.G.S.Venkatesan, "Finding the K-Edge connectivity in MANET using DLTRT, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5898 – 5904, 2014.
17. Ms. J.Praveena, K.G.S. Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.
18. K.G.S. Venkatesan. Dr. V. Khanna, "Inclusion of flow management for Automatic & dynamic route discovery system by ARS", International Journal of Advanced Research in computer science & software Engg., Vol.2, Issue 12, PP. 1 – 9, December – 2012.
19. Needhu. C, K.G.S. Venkatesan, "A System for Retrieving Information directly from online social network user Link ", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6023 – 6028, 2014.
20. K.G.S. Venkatesan, R. Resmi, R. Remya, "Anonymizimg Geographic routing for preserving location privacy using unlinkability and unobservability", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 523 – 528, March – 2014.
21. Selvakumari. P, K.G.S. Venkatesan, "Vehicular communication using Fvmr Technique", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6133 – 6139, 2014.
22. K.G.S. Venkatesan, G. Julin Leeya, G. Dayalin Leena, "Efficient colour image watermarking using factor Entrenching method", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 529 – 538, March – 2014.
23. Dr. K.P. Kaliyamerthie, K.G.S. Venkatesan, S. Sriram, N. Vijay, Richard Solomon, "Neighborhood based framework, Active Learning", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2535 – 2542, March -2015.
24. K.G.S. Venkatesan. Kausik Mondal, Abhishek Kumar, "Enhancement of social network security by Third party application", International Journal of Advanced Research in computer science & software Engg., Vol. 3, Issue 3, PP. 230 – 237, March – 2013.
25. V. N. Padmanabhan and R. H. Katz. TCP Fast Start: A Technique for Speeding Up Web Transfers. In Proc. IEEE Global Internet Conference (GLOBECOM), 1998.
26. K.G.S. Venkatesan, "Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August -2014.
27. B. Sundarraj, K.G.S. Venkatesan, Vimal Chand, "A Stochastic Model to Investigate Data center performance & QOS in IaaS cloud computing systems", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2560 – 2565, March -2015.
28. Anish Kumar Anbakarasan, Ilampiria Nagarajan, K.G.S. Venkatesan, "Moral Hacking : A way to boost data security by using vulnerability scanning Tools", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2605 – 2613, March -2015.
29. K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April 2013.
30. K.G.S. Venkatesan, "Automatic Detection and control of Malware spread in decentralized peer to peer network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 1, Issue 7, PP. 15157 – 15159, September -2013.
31. Satthish Raja, S K.G.S. Venkatesan, "Electronic Mail spam zombies purify in email connection", International Journal of Advanced Research in Computer Science Engineering & Information Technology, Vol. 1, Issue 1, PP. 26 – 36, June – 2013.
32. K.G.S. Venkatesan. Dr. V. Khanna, S.B. Amarnath Reddy, "Providing Security for social Networks from Inference Attack", International

Journal of Computer Science Engineering & Scientific Technology, March – 2015.

33. A.R. Arunachalam, K.G.S. Venkatesan, Abdul Basith.K.V., M. Sriram, "Traffic Identification Method Engine : An open platform for Traffic classification ",", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2475 – 2481, March - 2015.
34. K.G.S. Venkatesan, Dr. Kathir. Viswalingam, N.G. Vijitha, " Associate Adaptable Transactions Information store in the cloud using Distributed storage and meta data manager", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 1548 – 1555, March - 2015.
35. Abhinav Kumar, Abhijeet Kumar, Dr. C. Nalini, K.G.S. Venkatesan, "QOS – Guaranteed Neighbor selection & distributed packet scheduling algorithm by using MANET wireless networks", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2466 – 2474, March - 2015.
36. K.G.S. Venkatesan, Dr. V. Khanna, Jay Prakash Thakur, Banbari Kumar, "Mining User profile Exploitation cluster from computer program Logs", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 1557 – 1561, March - 2015.
37. Ms.J.Praveena, K.G.S.Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.
38. K.G.S.Venkatesan, "Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August -2014.
39. Margaret, A, & Henry, J., Journal of business ethics, Computer Ethics: The Role of Personal, Informal, and Formal Codes, 15(4), 425
40. K.G.S. Venkatesan, Dr. V. Khanna, S.B. Amarnath Reddy, "Network Monitoring using Test Packet Generation", IJSCONLINE, PP. 1-12, March – 2015.
41. F. Ye, S. Roy, and H. Wang, "Efficient Data Dissemination in Vehicular Ad Hoc Networks, " in IEEE J. on Sel. Areas in Comm., vol.30, no.4, pp.769-779, May 2012.
42. K.G.S. Venkatesan, Dr. V. Khanna, Dr. A. Chandrasekar, "Reduced path, Sink failures in Autonomous Network Reconfiguration System (ANRS) Techniques", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2566 – 2571, March - 2015.
43. L. Ghaderi, D. Towsley, and J. Kurose, "Reliability Gain of Network Coding in Lossy Wireless Networks, " in Proc. IEEE INFOCOM, Phoenix, AZ, Apr. 2008.
44. K.G.S. Venkatesan. Dr. V. Khanaa, Dr. A. Chandrasekar, "Autonomous System (AS) for mesh network by using packet transmission & failure detection", Inter. Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 12, PP. 7289 – 7296, December - 2014.
45. Sathish Raja, K.G.S. Venkatesan, "Electronic Mail spam zombies purify in E-mail connection", International Journal of Advanced Research in computer science Engineering & Information Technology, Vol. 1, Issue 3, pp. 28 - 36, June – 2013.
46. K.G.S. Venkatesan. Dr. V. Khanna, S.B. Amarnath Reddy, "Network Monitoring using Test Packet Generation", IJSCONLINE, PP. 1-12, March – 2015.
47. C. Fragouli, J. Widmer, and J. Le Boudec, "Efficient Broadcasting Using Network Coding, " in IEEE/ACM Trans. on Netw., vol.16, no.2, pp.450-463, Apr. 2008.