iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5322

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Secure Auditing for the Data Stored on Cloud by Third Party Auditor

Devaiah B M[1], Govind Yadav[2], Karthik H S[3], Madhu B R[4]
devaiah.b.m.25@gmail.com
[1, 2, 3. 4]*School of Engineering and Technology-Jain University*

Abstract: ***Distributed computing is a creating development that offers figure, accumulating and framework resources as an organization over the web. In coursed enrolling, information proprietors have their information on cloud servers and clients (information purchasers) can get to the information from cloud servers. In perspective of the information outsourcing, regardless, this new viewpoint of information empowering association in like way indicates new security challenges, which requires a self-speaking to separating relationship to check the data constancy in the cloud. Cloud customers can't depend just on cloud pro center for the security reasons of the outsourced data. The introduction of TPA murders the commitment of the client through the analyzing of whether his data set away in the cloud are undoubtedly set up, which can be basic in accomplishing economies of scale for Cloud Computing. Amidst examining, the customary information is kept private from open verifiers, who can check shared information respectability without downloading or recovering the whole information report. Presently we are presenting another plan by using and joining different compelling systems, and productive calculations accessible to guarantee the information of the client is secure. We lead the Experiment with different techniques and the think about the execution of the every strategy. The outcomes demonstrate that the proposed technique is secure and more productive as contrast with the current strategies as far as exhibitions. Elliptic Curve Cryptography Algorithm gives secure message uprightness and message approval, nearby non-disavowal of message and data protection. Cryptography is the best in class propels in the field of information security over to the framework.***

Keywords: ***Cloud Computing, encryption, elliptic curve cryptography, Third Party Auditor [TPA], Auditing***

I. INTRODUCTION

With the quick headway of capacity and preparing advancements, figuring assets have turned out to be more cheap, prevailing, and all around accessible than any time in recent memory. Distributed computing has been envisioned as the bleeding edge designing of huge business information industry. In distorted term Cloud enrolling is portrayed as securing and getting to data over the web instead of having in our PCs. It runs applications and organizations in a passed on outline with virtual resources. The applications and organizations are gotten to using a run of the mill web tradition. Distributed computing is a procedure in which figuring power, memory, structure can be passed on as an organization. A Cloud handling is a game plan of framework enabled organizations, guaranteed QoS, sensible figuring establishments on ask for with a straightforward and essential access. Cloud computing gives administrations which licenses clients to transfer their information remotely on cloud servers and access that information wherever around the system whenever. It gives numerous preferences; customer can store their records on cloud to maintain a strategic distance from the bother of putting away and maintaining the information documents locally. Likewise it gives information access from any topographical area and diminishes the equipment and programming support.

Data Owner who outsource the data on cloud can't have the vital resources for physically check the dependability of the outsourced data consequently he needs to trust on security traditions gave by CSP. Information protection, insurance of information, information accessibility, information area, and secure information transmission are a few issues that should be turned upward in cloud information security. The activity of physically evaluating the outsourced information can turn out to be particularly dreary occupation since the outsourced information is vast size. Information evaluating is another idea acquainted in Cloud processing with manage secure information stockpiling. Reviewing is a procedure of check of client information. It can be completed either by the client himself (information proprietor) or by a TPA. It keeps up the respectability of information put away on the cloud. To totally ensure on cloud client's information uprightness, it is huger to permit open reviewing administration for customer's outsourced information. Open reviewing administration makes utilization of an evaluator, for the most part a Third Party Auditor (TPA) whose activity is to as often as possible review the information documents transferred by information proprietor on cloud. These TPAs have information and skill that customers don't and are permitted to check the honesty of customer's outsourced records on cloud when required.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

A. Auditing

As the Service Level Agreement [SLA] isn't direct to the customers, there comes the need analysing to check for SLA encroachment. There are two sorts of investigating depending on which is being inspected: Internal Audit and External Audit. Inside Audit surveys the method that occurs in giving the organization. Outside Audit surveys the idea of organization, for instance, CPU execution, openness and SLA parameters. In case Cloud providers do assessing, they may cover their inadequacies and encroachment. On the other hand, if the customer does the looking at, it adds the overhead to them. The game plan is to have a third assembling substance to do the examining.

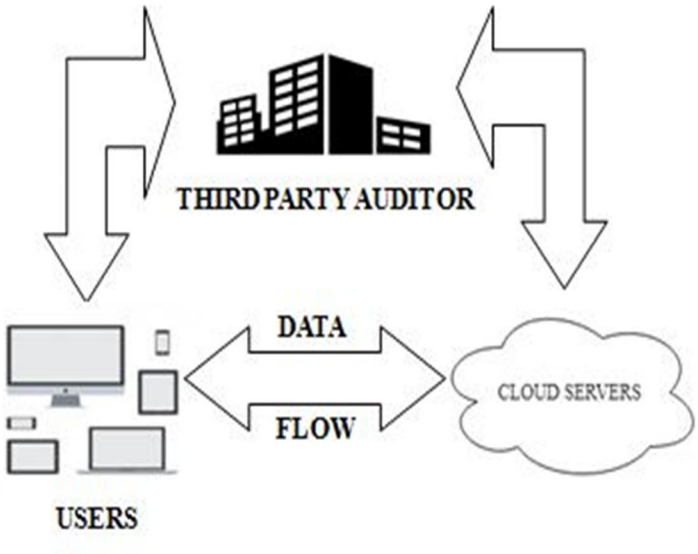


Fig. 1 Architecture of cloud data storage

B. Third Party Auditing [TPA]

Cloud specialist organizations regularly utilize Secure Socket Layer (SSL), Point to Point Tunnelling convention (PPTP), VPN for secure exchange. While exchanging the information amongst client and the cloud specialist organizations difficult to maintain a strategic distance from pernicious assault. In any case, clients require affirmation legitimately about the security over their information. The outsider screen the exercises of cloud client and cloud specialist organization. Ordinarily, cloud specialist co-ops and customer will have a Service Level Agreement (SLA).Service supplier needs to stick to rules specified in SLA independent of duties and offers gave to the client. The TPA Fig 2 will screen both the customer and specialist organization side exercises. There may emerge a circumstance where the specialist organization may erase the customer information, if not utilized for a drawn out stretch of time and there is no warning given to the customer with respect to this erasure. TPA proves to be useful in this circumstance, by advising the customer about the erasure that occurred in this manner keeping up a decent affinity between specialist co-op and customer. TPA will take after the evaluating standards and procedures, likewise they will have rundown of reviewing methodologies. As per the outsider review report, cloud specialist co-ops can screen the exercises of the client, if any client acting like the aggressor we can scratch off the assentation. The examining should be possible occasionally on tests of information. Over the period, the examples are gathered and confirmation is improved the situation the examples

The examining procedure comprises of three diverse kind of stages. Arranging, Execution and Reporting. In arranging stage the TPA need to conclude the accompanying vital undertakings, Content to review, Time timetable of the examining, length of evaluating, region of inspecting, review group estimate and so on. The review time and group survey relies upon the measure of the substance. Execution is the essential stages. In this stage we need to investigation the security dangers in the distributed storage, screen the past dangers and decide the level of past dangers. In like manner need to do the data genuineness check. Announcing is the report of execution stage, this report will enable the Cloud to specialist co-op to enhance their administration. The outsider review report specify the entire insights about the cloud client exercises and execution of the cloud specialist co-ops. As indicated by this review report Cloud Service Providers can screen the exercises of the client, if any client acting like the assailant we can scratch off the assentation. In the meantime Cloud Service Provider can enhance the administration effectiveness of the administration by this review report. Since this review report show the both client and cloud specialist co-op execution.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

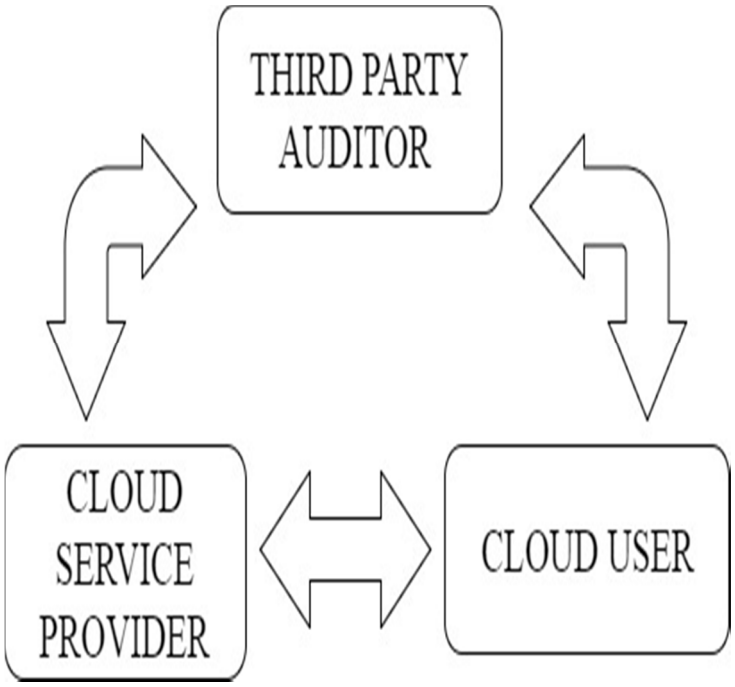


Fig .2 Third party auditor in cloud

C. ROLE OF TPA

The TPA procedure works in three stages: Key Generation, Server respectability confirmation, trustworthiness check. Key Generation: Key age is finished by the Owner. The information is encoded utilizing the private key of the proprietor and open key is exchanged alongside the information. Server Integrity evidence: TPA debate the server to give a proof of information uprightness. The server sends the verification. Uprightness Verification: On accepting the evidence from the Server, TPA checks the honesty without encoding the information. The tag in the information causes the TPA to check the information productively. The Auditing should be possible occasionally on tests of information. Over the period, the examples are gathered and confirmation is improved the situation the examples. This kind of inspecting falls under static classification. On confirmation if the inspector is persuaded with the information uprightness, the reviewer deletes the neighbourhood information.

II. PROBLEM STATEMENT

Due to multi-inhabitant attributes of the cloud, the ordinary security contraption are not any more appropriate for applications and information in cloud. A portion of the issue are as following:

A. All sorts of use and stuff of the cloud stage have no steady foundation and security limits simply because of dynamic adaptability, organization and region straightforwardness features of appropriated figuring model. In case of security infringement, it is hard to isolate a settled asset that has a risk or has been bargained.

B. Resources and cloud administrations might be hold by different suppliers as indicated by benefit serves models of Cloud processing. As there is a question of intrigue, it is hard to post a brought together safety effort.

C. Because of the transparency of cloud and sharing virtualized assets by multitenant, client information might be entered by other unlawful clients.

To determine these security matter numerous cryptography calculations are there.

The principal issue with data encryption in the cloud is making sense of who should play out the encryption and hold the key. If encryption keys are regulated by the CSP, count organizations can without a doubt be performed for CSU. In any case, CSPs are not for the most part solid and they can be related with disguising the data security scenes, (for instance, data setback or spillage) from the CSUs. This even ends up being most observably awful when CSP has toxic insiders who can manhandle the responsibility for keys by examining/changing/deleting or in spite of sharing the client's dubious data to an untouchable enemy.

In the distributed computing condition, the TPA is believed to be an exceedingly trusted assembling that can secure the assurance of the cloud customers. Then again, TPA can be a harmful insider to part the characterized information of the customer and pitch it to

various social occasions by taking the fix or diverse favourable circumstances for the exchanging of specific information. In this way, we require a tradition to choose the deceitful piece of TPA while auditing the records of the cloud customers. As, this area system gets dauntlessness the assessing method, yet it can extend the extra correspondence overhead. In this way, the light-weight dependable insurance defending tradition is required not solely to recognize the malevolent piece of TPA yet having minimum correspondence overhead.

III.LITERATURE REVIEW

As information is put away in server farm and is disseminated over the spots, which are far away to the customers, henceforth, it is critical to secure the information from outer and interior dangers. So in this situation distributed computing faces numerous issues in incorporating and securing the information. Henceforth, there is a requirement for procedures that will empower the honesty and secure the customers information. It is a troublesome assignment for cloud administration to give information security the same number of clients get to assets. TPA was acquainted with guarantee that the information put away on cloud is kept in place and diminishes client's contribution to certain degree.

Yanru Zhang, Xiang-Yang Li, and Zhu Han [2] proposed the idea of utilizing punishment to diminish CSP's motivation to cheat from an agreement hypothetical viewpoint, where cloud benefit clients can depend on an outside evaluator to check the calculation comes about when required.

J.Raja, Dr. M.Ramakrishnan [3] proposed security protection of information utilizing TPA administrations. It uses people in general key examining and arbitrary concealing techniques that guarantee that TPA couldn't see client's information amid the evaluating procedure. The proposed technique evacuates the weight of cloud clients from costly inspecting work.

M. Suguna and S. Kindness Shalinie [4] inspecting convention presents a put stock in outsider reviewer (TPA) will's identity accountable for checking the accuracy of information put away at distributed storage for the client without the requirement for recovering the whole information. The verification procedure in the proposed strategy diminishes the inspecting overhead at the cell phone utilizing short marks.

Anupriya.A.S, Ananthi, Dr. S Karthik [16] proposed an updated methodology for securing the TPA by utilizing Keyed Hash Message Authentication Code (HMAC).

Ms Bhavana Sharma [14] presents the Elliptic Curve Cryptography (ECC) system. Her work likewise states ECC can be utilized as a part of versatile registering, remote sensor systems, and server based encryption, picture encryption and its application in each field of correspondence et cetera. Dispersed processing with ECC is an absolutely new territory and has enormous degree of research.

M.S.Shashidhara , Jaini.C.P [23] proposed a sheltered distributed storage system which bolsters security safeguarding outsider examining. Furthermore, we consider the results to perform reviews simultaneously for various clients in a proficient way.

Akash Mishara, Nitin Rathod [6] proposed a plan where servers are required to work on determined lines for rightness.

Qian Wang [22] proposed the validation, confirmation and uprightness issues are unravelled through blowfish and hashing calculation.

Nirmaljeet Kaur, Harmandeep Singh [11] recommended that TPA is restricted to just giving the administration and utilizations hashing calculations for confirmation of information respectability and different calculations like AES, Blowfish for encryption and unscrambling.

Dalia Attas and Omar Batrafi [20] proposed a model for securing information without giving it and transferring any protected information to the cloud.

K. Govinda, E Sathiyamoorthy [17] strategy like Message Authentication Code [MAC] was utilized to confirm trustworthiness of information.

Tejashwini K, Sanjay Kumar C K [7] have proposed different strategies for securing information in cloud, which is delineated in Table1.

Afterward, fresher systems came into and an advanced mark is one of them

IV.METHODOLOGY

A. Existing System

Table 1 speaks to the different strategies with the confinements took after to secure the information through different instruments and they takes after as

Table 1 Existing various methodologies

METHODS ADOPTED	ADVANTAGES	DISADVANTAGES
With the use of multiple trusted Third party auditors.	Multiple auditors will handle most of the clients work and they are involved in auditing process also.	If in case the client's data is revealed to TPA then it will be a great failure.
With the use of RSA and MD5 algorithm.	There will be security enabled for the data stored in cloud.	If authentication system is corrupted or hacked then there will be a failure.
With the use of Homomorphic linear authentication system (HLA) and SHA-2.	Here in this the encryption process is more efficient and secure.	Here the auditor must regularly monitor the keys and there will be a online burden to clients also.
With the use of AES encryption algorithm.	Here greater efficiency is noticed in batch auditing by the auditor.	The complexity increases if the data in the cloud increases.
With the use of AAA security management	Here the fault tolerance will be provided by intelligence-based security.	The data redundancy is very my neglected.
With the use of BLS short signature	With the use of valid and accurate signature, the data can be recovered back.	This methodology fails if in case the message it self gets damaged.
With the use of Homomorphic authenticable ring Signature.	There is a support for block less verification for TPA.	There is failure if the servers are damaged and data is deleted.
With the addition of proxy servers.	Here each client's data is first verified, signed by the client, and added to cloud.	Here the single point failure or proxy threatens the security.

Different systems have been utilized like security saving evaluating convention. Barely any different calculations have likewise been utilized for effective examining of information put away on the cloud. Every one of them had certain downsides, so an effective and better strategy is to be proposed.

B. Proposed System

We have come up with a proposition of a system that is implemented using Advanced Encryption Standard [AES] [encryption], Secure Hash Algorithm [SHA-3][hashing] and Elliptic Curve Cryptography [Digital signatures].

In proposed framework we grew outsider inspector (TPA) which plans to confirm the uprightness of put away information. The framework comprises of three substances.

Cloud-It is worked by cloud pro centre (CSP) and gives esteemed storage space.

Social occasion people Two sorts of customer joined into get-together, one of a kind customer (OU) and number of get-together customers (GU). The primary customer is the proprietor of the data and offers data in get-together and gathering customers can get to that normal data.

TPA-Third Party Auditor-Third amassing assessor (TPA) can check the validity of shared information in light of enthusiasm from clients, without downloading the whole information.

Proprietor will store data record on the cloud server in sharable mode with get to approval. The functionalities related with outcast analyst are delineated in fig.3.

Just proprietor has make assent and assembling part has examined approval. Right when a customer (either the fundamental customer or a get-together customer) wishes to check the reliability of shared data, she at first sends a taking a gander at (uprightness) request to the TPA.

In the wake of enduring the investigating demand, the TPA produces a researching message (challenge) to the cloud server, and recovers a breaking down affirmation (demonstrate) of shared information from the cloud server. The TPA avows the rightness of the examining confirmation. At long last, the TPA sends a looking at report (uprightness answer) to the client in light of the result of attestation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

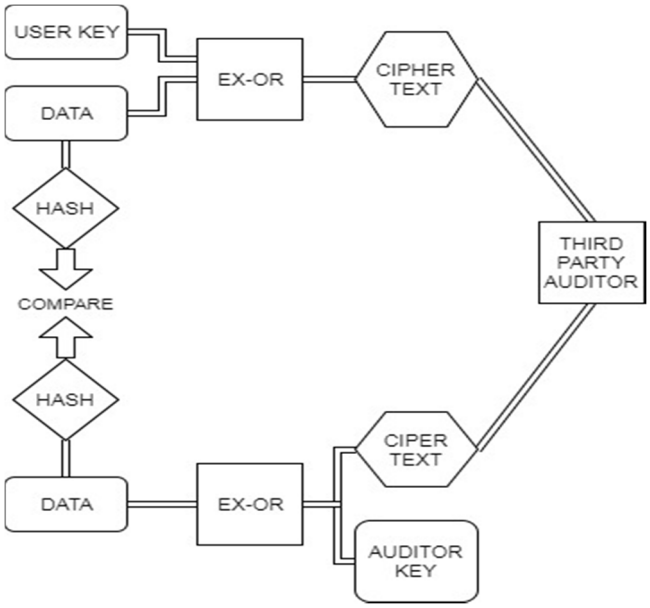


Fig. 3 Proposed system with third party auditor functionalities

AES has a key length of 128,192 and 256 bits and it is quite secure and has not been vulnerable to attacks, where the encrypted data has not been accessed.

SHA-3 has unlimited message size, it uses AND, XOR, NOT operations. It is a new addition to the SHA family. It is not vulnerable to brute -force attack. It has a different structure compared to SHA-2.

Elliptic bend has an exceptional property that makes it suitable for use in cryptography i.e. Its ability to take any two spotlights on a specific curve, incorporate them together and get a third point on a comparable twist. The rule errand related with ECC is point increment, i.e. enlargement of a scalar K with any immediate P on the curve toward gain another point Q on a comparative twist.

An elliptic twist is described by a condition, is of two variables, with coefficients. With the ultimate objective of cryptography, the variable and coefficients are confined to an uncommon kind of set called a FINITE FIELD. The general condition for an elliptic twist is:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Where a, b, c, d and e are bona fide numbers and x and y in like manner take their characteristics from honest to goodness number. An improved elliptic bend condition is given as:

$$y^2 – x^8 + dx + e$$

The TPA gathers the metadata and produce marks for every coalition k. At long last, the inspector confirms the marks and sends the outcomes to the client. The outcome contains points of interest of both approved and suspicious information squares. The documents will be encoded in the customer side and will be sent to the TPA utilizing open key-based encryption.

C. few Advantages of Utilizing ecc

1) Faster
2) Lower control utilization
3) Low CPU use
4) Low memory use
5) Shorter key size contrasted with RSA i.e., ECC=256bit while RSA=3072 bit
6) 10 times harder to split than RSA 2048.
7) Fast key age (no primality testing)
8) Faster decoding
9) Large SSL organizations with/without extra equipment

D. Signature Algorithm

Digital Signature Generation

For denoting a message m by sender of cloud A, using A's private key dA Digital Signature Verification
If B needs to authenticate A's signature, B must have A's open key pA.
Confirm that r and s are number in [1, n-1] .
Calculate e = HASH (m), where HASH () is a comparative limit used as a piece of the stamp age
Calculate w = (s– 1)%n
Calculate u1 = e*w % n and
u2=r*w % n
Calculate (x1, y1) = u1 * B + u2 * PA.
The signature is substantial if
x1=r % n, generally invalid.

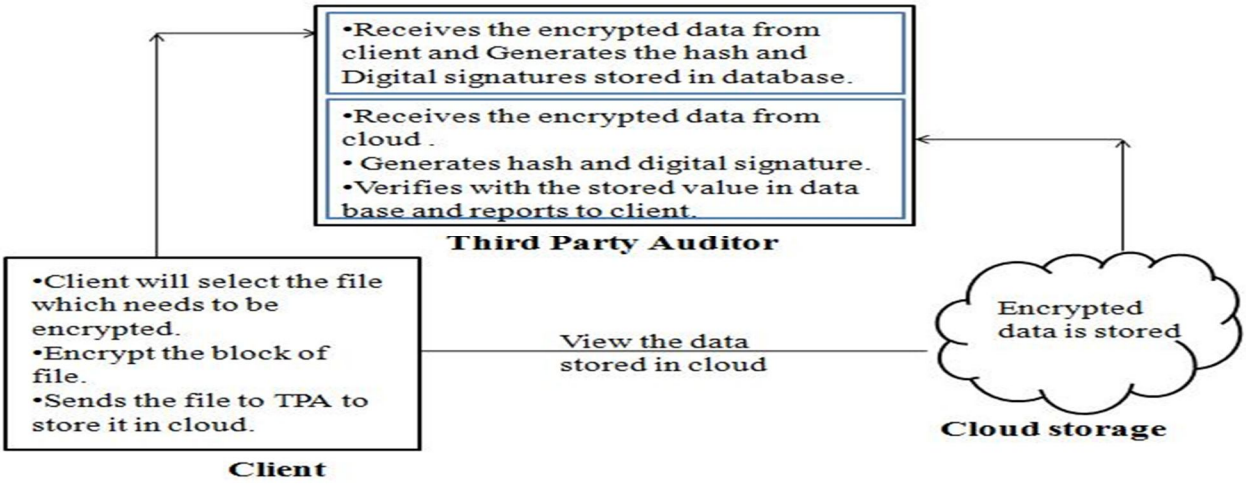


Fig. 4 Roles and Responsibilities

Fig. 4 depicts the roles and responsibilities of each entity in the architecture.

In the proposed system, certain steps are associated with the signature generation and verification process. Fig 5 depicts the signature generation process and Fig 6 depicts the signature verification.

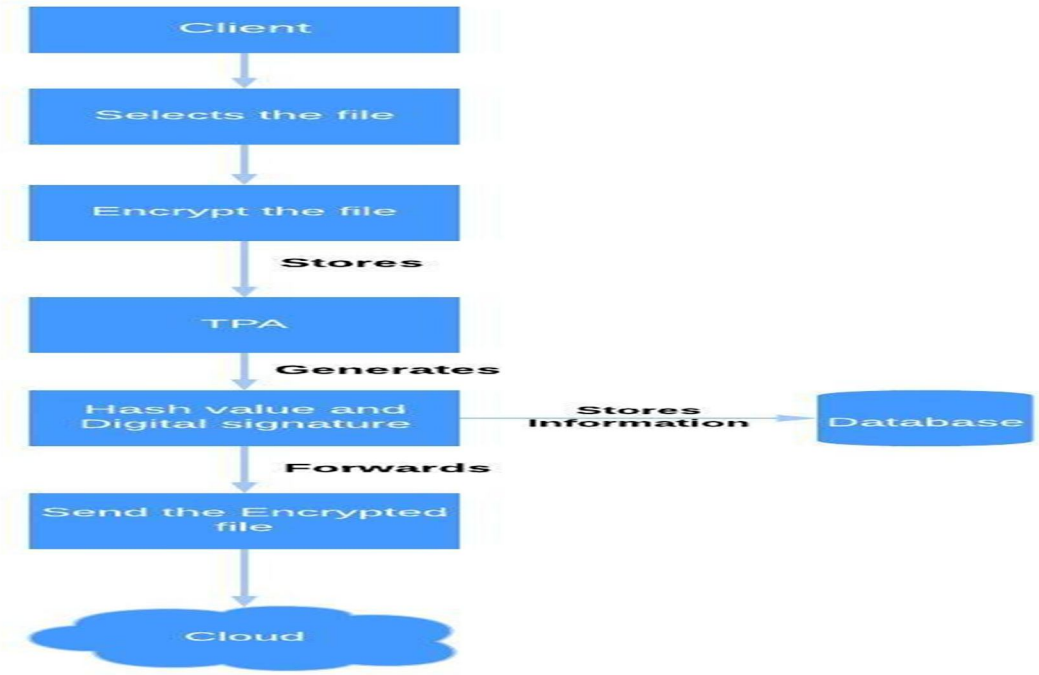


Fig .5 Work Flow Diagram for signature Generation

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

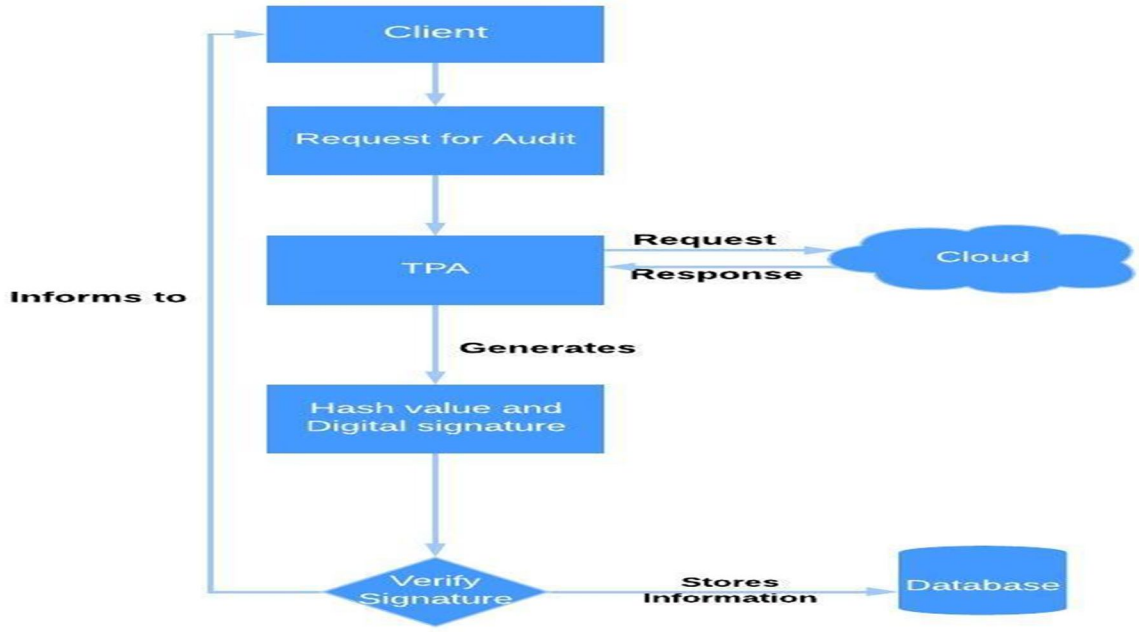


Fig. 6 Work Flow Diagram for signature Verification

In this manner, utilizing a mix of aes, sha-3 and ecc the framework is produced that gives better examining offices along these lines helping in securing the cloud information.

V. RESULTS

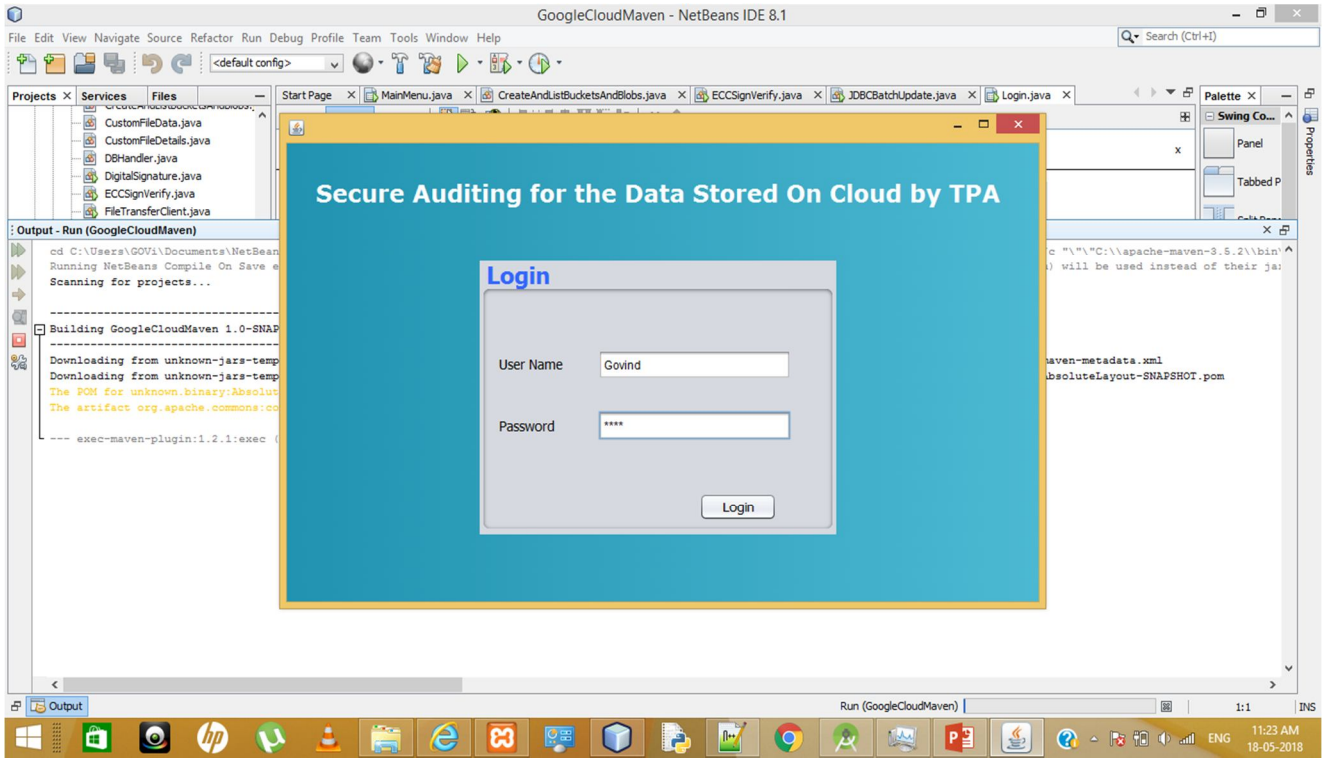


Fig 7. Login Page

Fig 7 depicts the login page of the TPA system interface where user has to enter the credentials in order to perform the required operations.

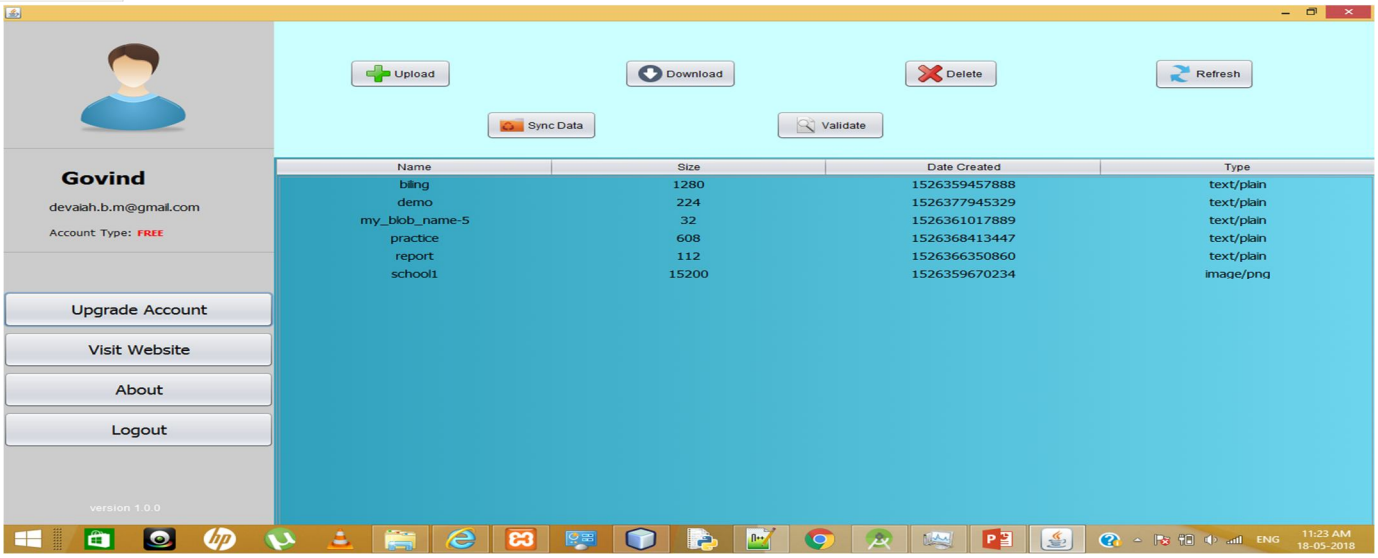


Fig 8 Home page

The home page consists of user details, account type and other details on the left, followed by various operations like update, delete, download and refresh.
The sync data operation helps to sync the data whenever it is modified by the user. The list of files present in the cloud is displayed along with the size, date of creation and file type.
All this is depicted in Fig 8.

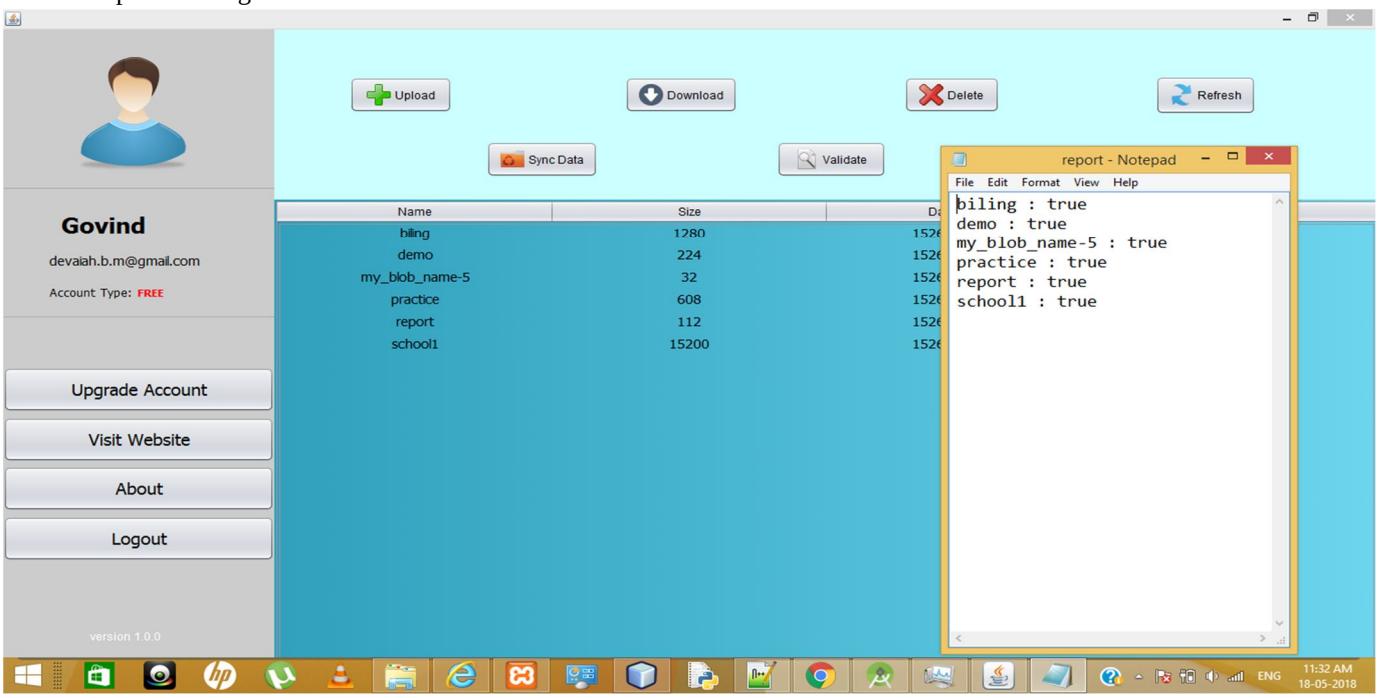


Fig 9 Report generated when validate function is used.

Validate is another function in the system, whenever the data is to be checked the validate operation can be performed and the report is generated for all the existing files. If the file is returned with false value it indicates that the file has been tampered, or there has been an attempt to modify the data. Fig 9 gives the report generated after the validate operation is performed.
Another feature that is included is the encryption where the files downloaded by the authenticated user through the system gets decrypted and the original data is obtained.

On the other hand if any attacker, hacker or any other random person tries to download the file from the cloud the file will be downloaded but contents will be encrypted making the data secure and the user also gets a report of this attack or unauthorized access.

It is observed that the system proposed is much more secure as it uses encryption, hashing as well as digital signatures.

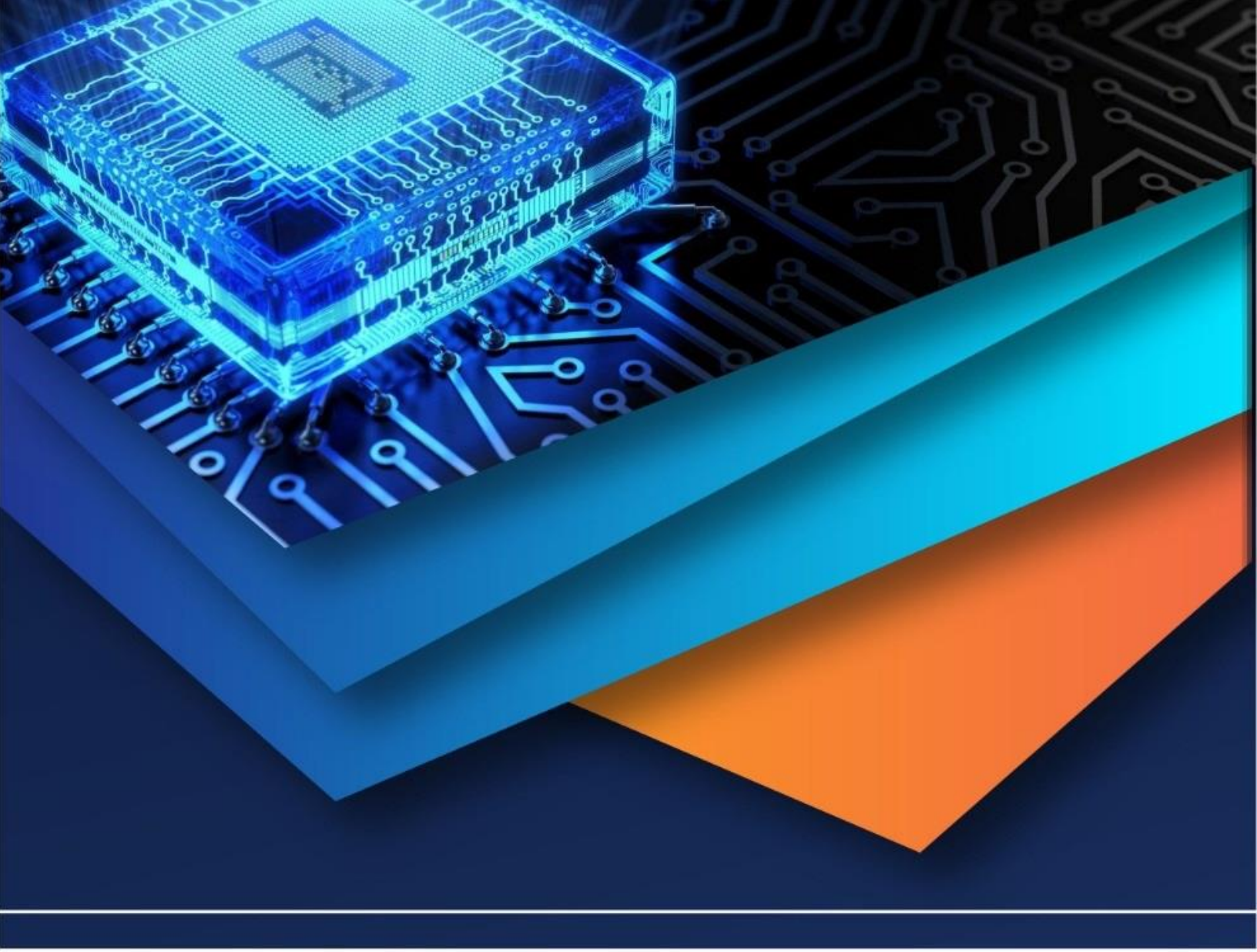
VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a structure that secures data on the cloud through the outcast evaluator. The TPA does the examining occasionally and in this way diminishing the weight of the customer. The weight of specialist organization to give better security is likewise lessened as TPA has a critical influence in it. The TPA screens both customer and specialist organization exercises. We have proposed a framework where the TPA utilizes the computerized signature alongside encryption/decoding calculations to improve the security of cloud information. The ECC signature calculation is considered as it furnishes a great deal of advantages alongside improved security contrasted with different techniques proposed. Along these lines, we hope to give a framework that gives improved security of cloud information. Distributed computing with ECC is a totally new area and has gigantic extent of research.

REFERENCES

[1] Debasis Das, “Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation”, 978-1-5386-2290-2/18/$31.00 ©2018 IEEE, ICOIN 2018.
[2] Yanru Zhang, Xiang-Yang Li, and Zhu Han, “Third Party Auditing for Service Assurance in Cloud Computing”, 978-1-5090-5019-2/17/$31.00 ©2017 IEEE
[3] J.Raja, Dr. M.Ramakrishnan, “Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment”, International Conference on Intelligent Computing and Control Systems ICICCS 2017.
[4] M. Suguna, S. Mercy Shalinie, “Privacy Preserving Data Auditing Protocol for Secure Storage in Mobile Cloud Computing”, IEEE WiSPNET 2017 conference.
[5] Jayashree Agarkhed, Ashalatha R., “An Efficient Auditing Scheme for Data Storage Security in Cloud”, 2017 International Conference on circuits Power and Computing Technologies [ICCPCT].
[6] Akash Mishara,Nitin Rathod, “Security in data storage on cloud environment using blowfish and digital signature”, International Journal of Research In Science & Engineering, e-ISSN: 2394-8299, Volume: 3 Issue: 2, March-April 2017 .

[7] Tejashwini K, Sanjay Kumar C K, "Methods for Secure Public Auditing in Cloud Storage", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), ISSN: 2347 - 8446 (Online) ISSN: 2347 - 9817 (Print), Vol. 4, Issue 2 (Apr. - Jun. 2016).
[8]Rahul K. Morghade, Sonal Honale, "Data storage security in cloud computing using third party auditor (TPA)", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, ISSN: 2277-9655, July, 2016.
[9] Ms. Kalyani B. Ghutugade, Prof. G. A. Patil, "Privacy preserving auditing for shared data in cloud", 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016.
[10] Swapnali S. More, Sangita S. Chaudhari, "Secure and Efficient Public Auditing scheme for Cloud Storage", 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016.
[11] Nirmaljeet Kaur, Harmandeep Singh, "Efficient and Secure Data Storage in Cloud Computing Through Blowfish, RSA and Hash Function", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 4 Issue 5, May 2015.
[12] Syed Rizvi, Katie Cover, Abdul Razaque, "Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment", 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing.
[13] Cong Wang, Sherman S.M. Chow, Qian Wang, , Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE transactions on computers, VOL. 62, NO. 2, February 2013.
[14] Ms Bhavana Sharma, "Security architecture of cloud computing based on elliptic curve cryptography (ecc)", Special Issue: Proceedings of 2nd International Conference on Emerging Trends in Engineering and Management, ICETEM 2013.
[15] Y Govinda Ramaiah, G Vijaya Kumari, "Complete Privacy Preserving Auditing for Data Integrity in Cloud Computing", 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications
[16] Anupriya.A.S, Ananthi, Dr. S Karthik, "Tpa based cloud storage security techniques", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 8, October 2012.
[17] K. Govinda, E.Sathiyamoorthy, "Data Auditing in Cloud Environment using Message Authentication Code", International Conference on Emerging Technology Trends on Advanced Engineering Research (ICETT'12) Proceedings published by International Journal of Computer Applications® (IJCA),2012.
[18] Kan Yang, Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2012 IEEE
[19] Reshma Suryawanshi, .Santosh Shelke, "Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme", 2012.
[20] Dalia Attas and Omar Batrafi, "Efficient Integrity Checking Technique for Securing Client Data in Cloud Computing", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05, October 2011.
[21] Dr. Kumar Parasuraman, Dr. P. Srinivasababu, S. Rajula Angelin and T. Arumuga Maria Devi, "Secured Document Management through A Third Party Auditor Scheme in Cloud Computing", 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE).
[22] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.
[23] M.S.Shashidhara, Jaini.C.P, "Privacy Preserving Third Party Auditing In Multi Cloud Storage Environment",2011.
[24] Cong Wang, Qian Wang, Kui Ren , Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY