RESEARCH REVIEW JOURNALS
Volume-03
Issue-05
May-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Concentration of Cloud Data Storage for Enhancement of Transmission Security

Shelja

Assistant Professor in Computer Science and Applications, R.S.D. College, Ferozepur City (India)

ARTICLE DETAILS

Article History
Published Online: 24 May 2018

Keywords
Cloud Computing, Decryption, Digital Signature, Encryption, Integrity, Message Digest, Cloud, Private Cloud, Security, Secure data Transmission

ABSTRACT

Data security has reliably been a noteworthy issue in information technology. In the cloud computing environment, it turns out to be especially genuine in light of the fact that the data is situated in better places even in the entire globe. Data security and access control is a standout amongst the most difficult continuous research work in cloud computing, because of clients outsourcing their delicate data to cloud suppliers. The different existing arrangements that utilization unadulterated cryptographic procedures to moderate these security and access control issues experience the ill effects of overwhelming computational overhead on the data proprietor and in addition the cloud service supplier for key appropriation and administration. Cloud storage moves the client's data to substantial data focuses that are remotely situated, on which client does not have any control. This novel component of the cloud postures numerous new security challenges which should be obviously comprehended and settled. Cloud Computing has been imagined as the cutting edge engineering of IT Enterprise. As opposed to conventional arrangements, where the IT services are under appropriate physical, coherent and staff controls, Cloud Computing moves the application programming and databases to the extensive data focuses, where the administration of the data and services may not be completely reliable. This remarkable characteristic, be that as it may, postures numerous new security challenges which have not been surely knew. In this article, we concentrate on cloud data storage and transmission security, which has dependably been an imperative part of nature of service. To guarantee the rightness of clients' data in the cloud, we propose a powerful and adaptable circulated conspire with two striking highlights, contradicting to its forerunners. Cloud storage empowers clients to remotely store their data and appreciate the on-request great cloud applications without the weight of nearby equipment and programming administration. This article explores the obstructions and answers for giving a reliable cloud computing environment.

1. Introduction

Security Secure Data transfer and Communication plays very important role in cloud computing. Cloud computing is a utilization of computer resources that are available on demand and access via a system. These services are broadly partitioned into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-aService (SaaS). The name cloud computing was roused by the cloud image that's frequently used to speak to the Internet in flowcharts and diagrams. Cloud computing is one of today's most sweltering research areas because of its ability to diminish costs associated with computing while at the same time increasing scalability and flexibility for computing services. Cloud computing has risen as the cutting edge technology which created in last couple of years, and is considered as the following enormous thing, in years to come. Since it is new, so it faces new security issues and new challenges as well. In the last couple of years it is grown up from simply being an idea to a major part of the IT business. Cloud computing is broadly accepted as the adoption of SOA, virtualization, and utility computing, it generally takes a shot at three sort of architecture and these are: SaaS, PaaS, and IaaS. There are distinctive issue and challenges with each cloud computing technology. Contrary to traditional computing practices, in a cloud computing environment, data and the application are controlled by the service supplier. This leads to a natural worry about the safety of the data and also its assurance from internal as well as external threats. Regardless of all these worries, advantages, for example, on demand infrastructure, diminished cost of maintenance, pay as you go, elastic scaling and so on are major reasons for undertakings to settle on cloud computing environments. Putting away of client data in the cloud regardless of its advantages has many fascinating security concerns which should be widely investigated for making it a reliable answer for the issue of avoiding local storage of data. All these various advantages offered by the cloud can be delighted in while utilizing services offered by a private cloud by paying a few charges however the same thing can be appreciated by utilizing an open cloud at the least cost or no cost. Be that as it may, utilizing open cloud services also accompanies an additional threat regarding the security of data put away at open cloud.

2. Security problem in cloud computing

In a typical scenario where an application is facilitated in a cloud, there are two broad security addresses that arise: – How secure is the Data? – How secure is the Code? Cloud computing environment is assumed as a potential cost saver as well as supplier of higher service quality. Security, Availability, Reliability, Data Integrity, Confidentiality, Access control, Authentication is the major quality worries of cloud

service clients. In one of the noticeable challenge among all other quality challenges.

3. Benefits of security in cloud computing

Current cloud service suppliers operate large systems. They have complex methods and master work constrain for maintaining their systems, which small enterprises may not have access. Thusly, there are many immediate and aberrant security advantages for the cloud customers. Here we display a bit of the main security advantages of a cloud computing environment:

Data Centralization

In a cloud environment, the cloud service supplier takes care of storage issues and small businesses require not spend a considerable measure of cash on physical storage devices. Cloud based storage gives a way to centralize the data in a faster and potentially cheaper manner. This is extremely valuable for small businesses, which cannot spend more cash on security parameters to secure the data.

Incident Response

IaaS suppliers can set up a dedicated forensic server that can be utilized on demand basis. As soon as, a security violation takes place in the cloud environment, the server can be brought on the web. In some investigation cases, even a backup of the environment can be easily made and put onto the cloud without affecting the normal course of business.

Forensic Image Verification Time

Some cloud storage implementations uncover a cryptographic check total or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm5)hash automatically when you store a question. Consequently in principle, the need to generate tedious MD5 checksums utilizing external devices is eliminated.

Logging

In a traditional computing paradigm all around, logging is viewed as an afterthought. Allocating lacking plate space makes logging either non-existent or minimal. Be that as it may, in a cloud, storage the requirement for standard logs is automatically solved.

4. Problem Statement

Cloud security is turning into a key differentiator and focused edge between cloud suppliers. By applying more grounded security methods and practices, cloud security may soon be more secure than the level that IT departments achieve utilizing their own hardware and software. A key obstacle to moving IT systems to the cloud is the lack of trust on the cloud supplier. The cloud supplier, thus, also needs to authorize strict security strategies, which thusly requires additional trust in the customers. To enhance the mutual trust amongst shopper and cloud supplier, a great trust foundation should be in place. Cloud computing can mean distinctive things to various individuals. The privacy and security concerns will unquestionably vary between a purchaser utilizing an open cloud application and a medium-sized venture utilizing a redid suite of business applications on a cloud platform and this brings an alternate package of advantages and dangers. What remains constant, however, is the real value that the client tries to ensure. For an individual, the value which is in danger can range from loss of common freedoms to the substance of bank accounts. For a business, the value keeps running from important trade insider facts to congruity of business operations and open reputation. A lot of this is very hard to estimate and translate into standard measurements of value. The task in this transition is to compare the chances of cloud adoption with the dangers associated with the same. In the event that cloud computing is so great, at that point for what reason isn't everybody doing it? Because the cloud act as a major black box nothing inside the cloud is noticeable to customer and this leads to two main issues that are : Integrity It is level of certainty that the data in the cloud is secured against accidential or intentional alteration without authorization. Consequently it infers that data ought to be sincerely put away on the cloud servers and any violation can be recognized. Privacy In this idea suppliers guaranteed that all critical data example charge card number are masked and just authorized clients have access for it. In 2009 a major occurrence in SAAS cloud happened with Google Docs. Google Docs allows clients to alter report on the web and share these records with different clients. In any case, once these records shared with any one it was accessible for everybody. Along these lines in era of personal privacy personal data should ensure.

5. Literature Survey

In 1990 the world was acquainted with the web and we began to see appropriated computing power realized on large scale. Today we have the ability to use scalable conveyed computing environment inside the limits of web, such a practice is known as cloud computing. As we already know there is loads of buildup associated with cloud computing. Cloud computing is a gigantic subject for that matter please take note of that we are as yet finding many security issues which will challenge to cloud computing because cloud computing is still work in advance and it is rapidly developing. Amid a keynote discourse to the Brookings Institution arrangement gathering, cloud Computing for Business and Society,Microsoft General Counsel Brad Smith also featured data from an overview authorized by Microsoft measuring attitudes on cloud computing among business leaders and the general population. The review found that while 58 percent of the general population and 86 percent of senior business leaders are amped up for the potential of cloud computing, however more than 90 percent of these same individuals are worried about the access, security and privacy of their own data in the cloud.

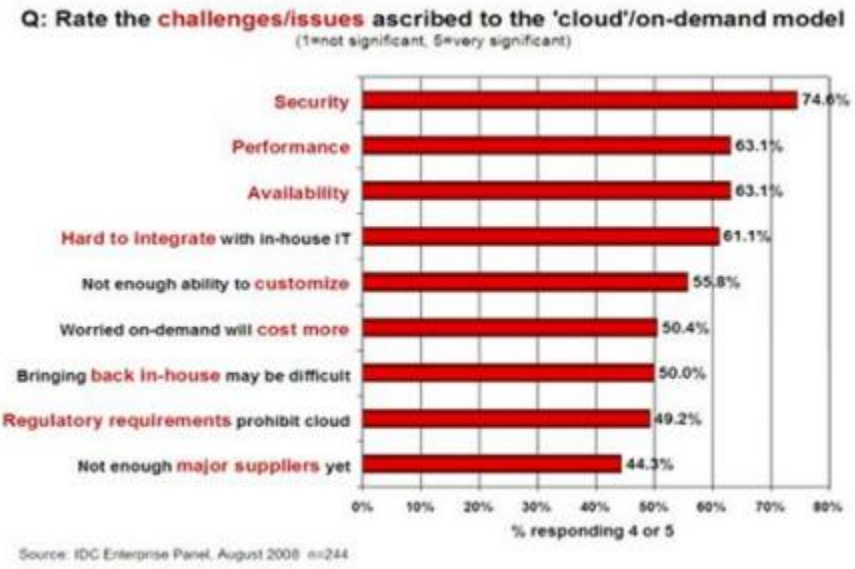

Figure 1: Survey showing issues related to cloud

As we experience the graph of rate of issues and challenges over cloud it demonstrates that security is all the more demanding as compared to other issuesIn the author says that the US National Institute of Standards and Technology (NIST), an agency of the Commerce Department Technology Administration, has created a cloud computing security gathering. This gathering considers its part as advancing the successful and secure utilization of the technology inside government and industry by giving technical guidance and advancing standards NIST has as of late released its draft wide to adopting and utilizing the Security Content Automation Protocol which distinguishes a very of specifications for organizing and communicating security-related information in standard ways, as well as related data, for example, identifiers for software flaws and security configuration issues. Its application incorporates maintaining venture systems security. In addition to NIST endeavors, the industry itself can affect an undertaking approach to cloud security. On the off chance that there is application of due persistence and advancement of an approach of self-regulation to guarantee that security is adequately executed among all clouds, at that point this arrangement can also help in facilitating law-making. By joining industry best practices with the oversight NIST and different substances are as yet creating, we can adequately address cloud computing future security needs. In a prologue to cloud computing has been exhibited that is relied upon to be adopted by the administrations, manufacturers and the academicians in the exact near future. The author also provides an overall insight of all current strategies for cloud data security and techniques proposed for guaranteeing data authentication utilizing TPA. In the author elaborates the various unresolved issues threatening cloud computing adoption and affecting the various stake-holders associated with it. The author exhibits an approach which is aimed at building up an understanding of the security threats that hamper the security and privacy of a client. The various characteristics of a protected cloud infrastructure (open or private) have been examined and also its challenges and the ways to explain them. The author also features various security concerns related to the three basic services gave by a Cloud computing environment and the answers for avoid them. In the author has worked towards facilitating the customer in getting a proof of integrity of the data which he wishes to store in the cloud storage servers with bare least expenses and endeavors. The plan was proposed by the author to lessen the computational and storage overhead of the customer as well as to limit the computational overhead of the cloud storage server. In author recommends authentication and encryption for secure data transmission from one cloud to other cloud that requires secure and authenticated data with elliptic bend cryptography. The author has made utilization of Elliptic bend cryptography to give confidentiality and authentication of data between clouds. In author considers the cloud environment as another computing platform to which the classic strategy of security research can be applied. The author decides to utilize an attribute-driven philosophy to lead their survey. In the author analyses the basic issue of cloud's data security. With the analysis of the architecture of HDFS, they get the data security necessities of cloud computing and set up a mathematical data demonstrate for cloud computing.

6. Proposed Work

Creating Web Application For Campus Management

As a matter of first importance, the Admin of the online interface would check its clients. The clients who can access this web application from program are Student, TPO, and HR. On the off chance that the client is confirmed effectively the admin would approve the particular client. After the school TPO or company admin have been approved now the school TPO can thusly approve the undergrads. All these clients access application which is placed over "APPLICATION SERVER". Application server is safe server. All security credentials are put away in application server. It is accessed by trusted individual say Third Party Auditor (TPA) after regular intervals of time. Data of this web application will be put away finished "DATABASE" server (public cloud). Data will be transferred from Application server to Database Server. Our proverb is to secure the data transfer from one cloud (i.e. application server) to other cloud (i.e. database server). We will maintain data integrity and privacy utilizing our solid security

mechanism. Data will be scrambled utilizing public key of database server and sent to database server. While recovering data database server will send data to application server by encoding data by individual client's public key.

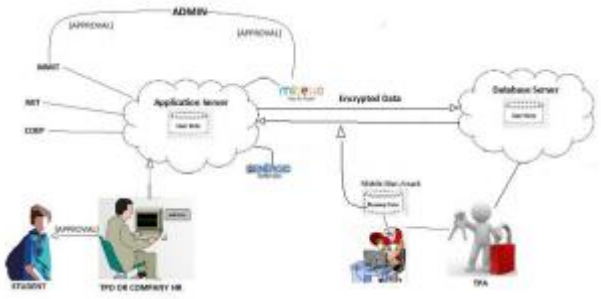

Figure 2: Architecture

So if company will have their some choice criteria process that is 60 percent or 50 percent at that point according to that they will fire the question and will get the rundown of meriting candidate. Between all these transaction there can be a man or a center man attacker who can exchange the real data put away on cloud with his spurious data and false information can be given to the company

Secure data transfer from cloud to cloud

Let us assume that we have two organizations A and B. A and B act as public clouds with data, software and applications. A want to send data to B's cloud securely and data should be authenticated.

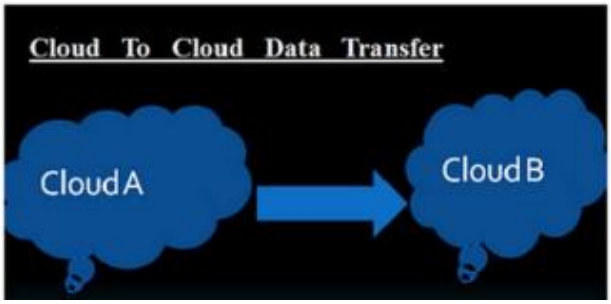

Figure 3: Data Transfer

We are here attempting to send a safe data from A to B by applying digital signature and data encryption. Assume B wants a XML report from A's cloud at that point B's client will place a demand to A's client. A's client select relating XML record from A's cloud data storage and then apply the hash work, it will give message process. Sign the message process with his private key by utilizing A's software. It is called digital signature. Scramble digitally marked signature with B's public key. Encoded figure message will be send to B. B's software decode the figure message to XML report with his private key and check the signature with A's public key. 5.3File Transfer in File Transfer Module, understudies can upload their resume, certificates and images while filling understudies academic information frame. Those records will be transmitted in scrambled format and will be put away in cloud in plain content format. At whatever point company wants to choose the understudies for enrollment process, they will fire the question based on criteria then they will get the rundown of meriting understudies. They can also download the resume of chose understudy for review extra information related to them. Attacks on File As there is have to give security to the data, there is also need to give security to the uploaded document. This is because attacker can attack the document and he will able to do following various sorts of attacks:-

Reading substance of document.

Survey and duplicating of image show in continue.

Attacker can also adjust the substance of document.

Attacker can abuse the authorized archives like Certificates.

7. Data Integrity

Data integrity is a standout amongst the most critical elements in any information framework. Generally, data integrity means shielding data from unauthorized cancellation, modification, or fabrication. Managing element's admittance and rights to particular endeavor resources guarantees that valuable data and services are not abused, misappropriated, or stolen. Data integrity is easily achieved in a standalone framework with a solitary database. Data integrity in the standalone framework is maintained via database constraints and transactions, which is usually wrapped up by a database management framework (DBMS). Transactions ought to take after ACID (atomicity, consistency, isolation, and durability) properties to guarantee data integrity. Most databases bolster ACID transactions and can protect data integrity. Authorization is utilized to control the access of data. It is the mechanism by which a framework figures out what level of access a particular authenticated client ought to have to secure resources controlled by the framework. Data integrity in the cloud framework means saving information integrity. The data ought not be lost or changed by unauthorized clients. Data integrity is the basis to give cloud computing service, for example, SaaS, PaaS, and IaaS. Other than data storage of large-scaled data, cloud computing environment usually gives data preparing service. Data integrity can be obtained by methods, for example, RAID-like strategies and digital signature. Attributable to the large quantity of substances and access focuses in a cloud environment, authorization is crucial in assuring that lone authorized elements can interact with data. By avoiding the unauthorized access, organizations can achieve greater trust in data integrity. The checking mechanisms offer the greater perceivability into figuring out who or what may have altered data or framework information, potentially affecting their integrity. Cloud computing suppliers are trusted to maintain data integrity and accuracy. Nonetheless, it is necessary to manufacture the third party supervision mechanism other than clients and cloud service suppliers. Checking the integrity of data in the cloud remotely is the perquisite to convey applications. Arbors et al. proposed a theoretical framework "Confirmations of Retrievability" to realize the remote data integrity checking by joining mistake adjustment code and spot-checking. The HAIL framework utilizes POR mechanism to check the storage of data in various clouds, and it can guarantee the redundancy of various duplicates and realize the availability and integrity checking. Schiffman et al. proposed put stock in platform module (TPM) remote checking to check the data integrity remotely.

8. Data Confidentiality

Data confidentiality is important for clients to store their private or confidential data in the cloud. Authentication and access control strategies are utilized to guarantee data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and dependability. Because the clients don't confide in the cloud suppliers and cloud storage service suppliers are virtually difficult to eliminate potential insider threat, it is extremely dangerous for clients to store their touchy data in cloud storage straightforwardly. Straightforward encryption is faced with the key management issue and cannot bolster complex prerequisites, for example, inquiry, parallel modification, and fine-grained authorization.

9. Homomorphic Encryption

Encryption is usually used to ensure the confidentiality of data. Homomorphic encryption is a kind of encryption system proposed by Rivest et al.

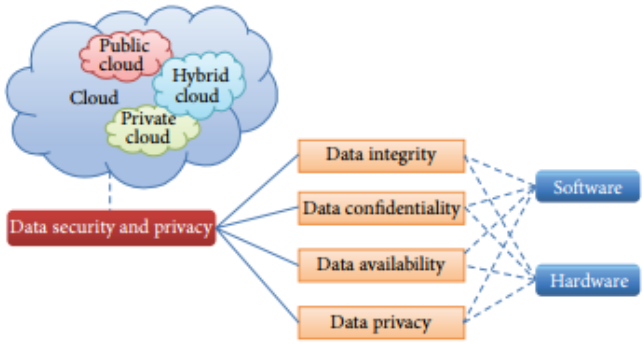

Figure 4: Organization of data security and privacy in cloud computing

It guarantees that the figure content algebraic operation comes about are reliable with the clear operation after encryption comes about; in addition, the entire procedure does not have to unscramble the data. The implementation of this procedure could well explain the confidentiality of data and data operations in the cloud. Upper class right off the bat proposed the completely homomorphic encryption strategy, which can do any operation that can be performed in clear content without unscrambling. It is an important breakthrough in the homomorphic encryption technology. Notwithstanding, the encryption framework includes exceptionally complicated calculation, and the cost of computing and storage is high. This leads to the fact that the completely homomorphic encryption is still far from real applications. A cryptographic algorithm named Diffie-Hellman is proposed for secure communication, which is very dissimilar to the key dissemination management mechanism. For greater flexibility and enhanced security, a mixture method that consolidates different encryption algorithms, for example, RSA, 3DES, and random number generator has been proposed . RSA is helpful for establishing secure communication association through digital signature based authentication while 3DES is particularly valuable for encryption of piece data. Furthermore, several encryption algorithms for guaranteeing the security of client data in the cloud computing are examined.

10. Encrypted Search and Database

Because the homomorphic encryption algorithm is wasteful, researchers swing to ponder the applications of restricted homomorphic encryption algorithm in the cloud environment. Encoded search is a typical operation. Manivannan and Sujarani have proposed a lightweight mechanism for database encryption known as transposition, substitution, collapsing, and moving (TSFS) algorithm. Be that as it may, as the quantities of keys are increased, the amount of computations and handling also increases. In-Memory Database encryption strategy is proposed for the privacy and security of delicate data in untrusted cloud environment. A synchronizer exists between the proprietor and the customer for looking for access to the data. Customer would require a key from the synchronizer to decode the encoded shared data it gets from the proprietor. The synchronizer is used to store the correlated shared data and the keys separately. An inadequacy of this procedure is that the delays happen because of the additional communication with the central synchronizer. In any case, this limitation can be mitigated by adopting bunch encryption and through limiting communication amongst hubs and synchronizer. Huang and Tso proposed an asymmetric encryption mechanism for databases in the cloud. In the proposed mechanism, the commutative encryption is applied on data more than once and the request of public/private key utilized for encryption/unscrambling does not make a difference. Reencryption mechanism is also utilized as a part of the proposed plot which demonstrates that the figure content data is scrambled by and by for duality. Such plans are exceptionally helpful in the cloud applications where privacy is a key concern. A privacy-protecting multikeyword ranked search approach over encoded cloud data was proposed, which can search the scrambled cloud data and rank the search comes about without leakage of the client's privacy.

11. Distributive Storage

Distributive storage of data is also a promising approach in the cloud environment. AlZain et al. talked about the security issues related to data privacy in the cloud computing including integrity of data, interruption, and availability of service in the cloud. To guarantee the data integrity, one choice could be to store data in various clouds or cloud databases. The data to be shielded from internal or external unauthorized access are partitioned into chunks and Shamir's mystery algorithm is utilized to generate a polynomial capacity against each piece. Ram and Sreenivaasan have proposed a procedure referred to as security as a service for securing cloud data. The proposed system can achieve maximum security by separating the client's data into pieces. These data chunks are then encoded and put away in separated databases which take after the idea of data dispersion over cloud. Because each section of data is scrambled and separately appropriated in databases over cloud, this gives enhanced security against various sorts of attacks. Arfeen et al. depict the dissemination of resources for cloud computing based on the tailored active measurement. The tailored measurement strategy is based on the network plan and the particular courses for the approaching and active traffic and gradually changing the resources according to the client needs. Tailored measurement relies upon the computing

12. Data Privacy

Privacy is the ability of an individual or gathering to detach themselves or information about themselves and along these lines reveal them specifically. Privacy has the accompanying elements.

When: a subject may be more worried about the present or future information being revealed than information from the past.

How: a client may be comfortable if his/her companions can manually ask for his/her information, however the client dislike alerts to be sent automatically and every now and again.

Extent: a client may rather have his/her information revealed as an ambiguous district rather than an exact point. In trade, customer's specific circumstance and privacy should be ensured and utilized appropriately. In organizations, privacy entails the application of laws, mechanisms, standards, and procedures by which personally identifiable information is managed. In the cloud, the privacy means when clients visit the delicate data, the cloud services can keep potential adversary from construing the client's behavior by the client's visit demonstrate (not immediate data leakage).

Researchers have concentrated on Oblivious RAM (ORAM) technology. ORAM technology visits several duplicates of data to shroud the real going by aims of clients. ORAM has been broadly utilized as a part of software security and has been utilized as a part of ensuring the privacy in the cloud as a promising technology. Stefanov et al. suggested that a path ORAM algorithm is state-of-the-art implementation. The privacy issues contrast according to various cloud scenarios and can be partitioned into four subcategories as takes after:

how to enable clients to have control over their data when the data are put away and prepared in cloud and avoid robbery, nefarious utilize, and unauthorized resale,

(ii) how to guarantee data replications in a purview and predictable state, where replicating client data to various suitable locations is a usual decision, and avoid data misfortune, leakage, and unauthorized modification or fabrication,

(iii) Which party is in charge of guaranteeing legal prerequisites for personal information?

(iv) To what degree cloud subcontractors are associated with preparing which can be appropriately distinguished, checked, and ascertained.

Service Abuse.

Service abuse means that attackers can abuse the cloud service and acquire extra data or pulverize the interests of different clients. Client data may be abused by different clients. Deduplication technology has been broadly utilized as a part of the cloud storage, which means that the same data frequently were put away once yet shared by various distinctive users.This will lessen the storage space and chop down the cost of cloud service suppliers, however attackers can access the data by knowing the hash code of the put away records. At that point, it is conceivable to leak the touchy data in the cloud. So verification of possession approach has been proposed to check the authentication of cloud clients. Attackers may lead to the cost increase of cloud service. Fraudulent asset utilization is a sort of attack on the payment for cloud service. Attackers can expend the particular data to increase the cost for cloud service payment. Idziorek et al. proposed this inquiry and researched on the recognition and identification of fraud asset utilization.

Averting Attacks

The cloud computing facilitates tremendous amount of shared resources on the Internet. Cloud systems ought to be capable of averting Denial of Service (DoS) attacks. Shen et al. analyzed prerequisite of security services in cloud computing. The authors propose integrating cloud services for confided in computing platform (TCP) and trusted platform bolster services (TSS). The trusted model should bear characteristics of confidentiality, dynamically fabricating put stock in domains and dynamic of the services. Cloud infrastructures require that client transfers their data into cloud just based on trust. Neisse et al. analyzed apathetic attacks scenarios on Oxen cloud platform to evaluate cloud services based on trust. Security of data and trust in cloud computing is the key point for its broader adoption. Yeluri et al. concentrated on the cloud services from security perspective and investigated security challenges in cloud while conveying the services. Character management, data recuperation and management, security in cloud confidentiality, put stock in, perceivability, and application architecture are the key focuses for guaranteeing security in cloud computing.

Identity Management

Cloud computing gives a platform to utilize extensive variety of Internet-based services. Be that as it may, other than its advantages, it also increases the security threat when a trusted third party is included. By including a trusted third party, there is a chance of heterogeneity of clients which affects security in the cloud. A conceivable answer for this issue could be to utilize a trusted third party autonomous approach for Identity Management to utilize character data on untrusted has. Squicciarini et al. concentrated on issues of data leakage and loss of privacy in cloud computing . Distinctive levels of securities can be utilized to avert data leakage and privacy loss in the cloud. Cloud computing gives new business services that are based on demand. Cloud networks have been worked through dynamic virtualization of hardware, software, and datasets. Cloud security infrastructure and the trust reputation management play a vital part to upgrade the cloud services. The Internet access security, server access International Journal of Distributed Sensor Networks 7 security, program access security, and database security are the main security issues in the cloud.

13. Conclusion

At last the conclusion of this paper present solid security techniques to secure the data files of a data proprietor in the cloud infrastructure .In our proposed plot, we have mainly endeavored to maintain the integrity and privacy of the put away data. The public key, hash, and private key figures utilized between the sender and collector guarantee a secure

environment at the cloud. Future augmentations incorporate leading an online aptitude test for the qualified understudies and giving security to the same. We trust that data storage security in Cloud Computing, an area brimming with challenges and of paramount importance, is still in its infancy now, and many research issues are yet to be recognized. Adding secure cloud storage utilizing the proposed cryptographic arrangement and with a searchable encryption system for the files to be accessed, it will work as a superior approach to the client to guarantee security of data. The cloud security utilizing cryptography is already being used for secure data storage which can be enhanced for secure data transmission and storage. A fascinating inquiry in this model is whether we can build a plan to achieve both public verifiability and storage rightness assurance of dynamic data. Moreover, along with our research on dynamic cloud data storage, we also plan to investigate the issue of fine-grained data mistake localization.

References

1. Veerraju Gampala. Data security in cloud computing with elliptic curve cryptography. International Journal of Soft Computing and Engineering (IJSCE), 2, 2012.
2. Zhifeng Xiao and Senior Member Yang Xiao. Security and privacy in cloud computing. IEEE COMMUNICATIONS SURVEYS and TUTORIALS,
3. Lori M. Kaufman John Harauz. Data security in the world of cloud computing. IEEE Computer and Reliability society, August
4. Party Auditor Indrajit Rajput. Enhanced data security in cloud computing with third party auditor. International Journal of Advanced Research in Computer Science and Software Engineering, 3.
5. Jens-Matthias Bohli.Security and privacy-enhancing multicloud architectures.
6. Amit Sangroya. Towards analyzing data security risks in cloud computing environments. JULY/AUGUST 2010.
7. Ashutosh Saxena Sravan Kumar R. Data integrity proofs in cloud storage. 2011..
8. Gu Yaqiang Zhang Quan Tang Chaojing Dai Yuefa, Wu Bo. Data security model for cloud computing. November 21-22, 2009.
9. N. Leavitt, “Is cloud computing really ready for prime time?” Computer, vol. 42, no. 1, pp. 15–25, 2009.
10. P. Mell and T. Grance, “The nist definition of cloud computing,” National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.
11. F. Berman, G. Fox, and A. J. G. Hey,Grid Computing: Making the Global Infrastructure a Reality, Volume 2, John Wiley and sons, 2003.
12. M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” IACR Cryptology EPrint Archive, vol. 186, 2008.
13. Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.
14. N. Kshetri, “Privacy and security issues in cloud computing: the role of institutions and institutional evolution,” Telecommunications Policy, vol. 37, no. 4-5, pp. 372–386, 2013.
15. R. Latif, H. Abbas, S. Assar, and Q. Ali, “Cloud computing risk assessment: a systematic literature review,” in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014.
16. Avizienis, J. Laprie, B. Randell, and C. Landwehr, “Basic ˇ concepts and taxonomy of dependable and secure computing,” IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

