Assurance on Data Integrity in Cloud Data Centre Using PKI Built RDIC Method

Arulkumar Venkatachalam, N Balaji
SSN College of Engineering
Kalavakkam. India
{it.arul@gmail.com} {drnbhalaji@gmail.com}

ABSTRACT: *A great deal of advances in innovation has offered fame to Cloud computing. It has turned into the most every now and again use answer for undertakings that need to focus on their data transactions and bit less worry on their infrastructures. Yet at the same time a few enterprises are not utilizing cloud facilities. The studies delights that security threats are the motivation behind why cloud computing isn't utilized as a specified goal. Cloud ventures questions security threats of the cloud. There are various kinds of security challenges for Cloud infrastructure. Such threats are identified as confidentiality, integrity, availability, accountability and privacy. In this work, we focus on the information integrity as characteristic of security. Since, in the wake of putting away information to cloud, client doesn't have even an inkling where the information is put away. The client's information should be put away in verified way. Hence, the proposed method PKI based RDIC concept to ensure the correctness of stored in cloud with the help of third party verifier.*

Keywords: Cloud Security, Data Integrity, Public Key Infrastructure

DOI: 10.6025/jisr/2020/11/1/10-20

Received: 27 October 2019, Revised 12 December 2019, Accepted 21 December 2019

1. Introduction

Cloud computing, which has gotten impressive consideration from research communities in the academia just as industry in a disseminated calculation model over a huge pool of shared-virtualization figuring assets. Presently the Cloud services, in straight-forward words is the name of conveying computing services over the cloud or the web. The computing services depict as systems administration, servers, databases, storage, programming, applications, infrastructure and the sky is the limit from there. Cloud suppliers who give these facilities over the web charge for their services according to use premise. For example, Storage, Computing power, deployed applications and services. Cloud clients are provisioned and discharge resources as they need in distributed shared computing condition. Various distributed storage administrations have risen to offer information redistributing for information proprietor e.g., SkyDrive, Dropbox, Zip cloud, One drive. Subsequently, clients can pick their fulfilled cloud storage suppliers as per access speed, security, dependability, cost and so forth. Hence 96% of organizations already use some form of the cloud storage, on average, businesses leverage nearly five separate clouds and over 26% of enterprises spend over $6 million per year on public cloud data centers. Consequently 96% of enterprises as of now utilize some type of the distributed storage, by and large, organizations influence almost five separate clouds and over 26% of ventures spend over $6 million every year on open cloud server farms. Cloud computing accompanies its own difficulties, however. As of now, assessments indicates that 35% of cloud spending goes to squander because of lacking cloud cost improvement. What's more, as applications, service managements and platforms keep on developing, IT administrators should be prepared to adjust.

2. Characteristics of Cloud Computing

The word cloud speaks to as the web or between associated PC frameworks or just a mammoth system framework. Cloud (Data Centers) exists at certain remote areas for the most part escaped the client, the client doesn't have even an inkling where his information is spared. It is giving numerous facilities over the web or over the network system, for example, public network systems and private network systems, for instance, Local Area Network (LAN), Wide Area Network (WAN) or even Virtual Private Network (VPN). Web Conferencing, Customer Relationship Management (CRM), Email and so forth are the utilizations of Cloud, and so on.

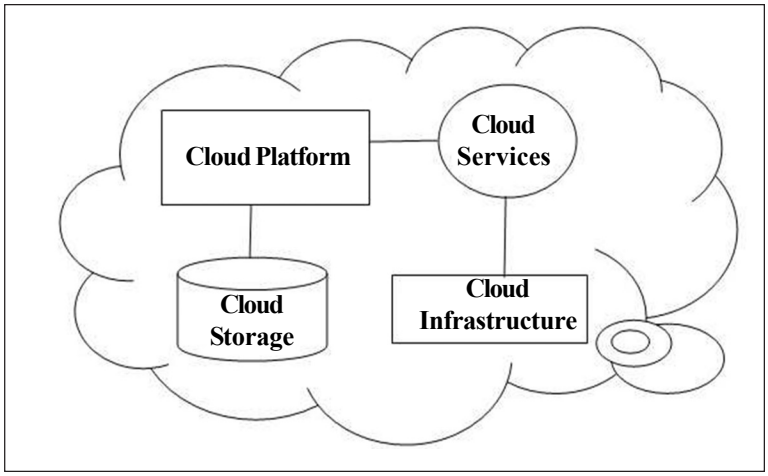

Figure 1. Cloud Architecture

On enduring, cloud computing is an IT model that conveys process control, extra storage unit, applications, and different assets on interest. The outcome is a pay as-you-go financial model that advances speed and deftness in IT activities. Furthermore, the far reaching movement to the cloud decreases (and regularly disposes of) the requirement for complex, on-premises equipment that require noteworthy assets to keep up.Cloud computing is regularly arranged dependent on two measurements such as based on location of the cloud and types of services it could offered. Based on locations, cloud environments shape into public,private and hybrid cloud. In public, at the point when the services are rendered over a system that is open for common use. Public cloud services might be free. This cloud makes it simple to access cloud facilities to the general population. The Private cloud is available just inside an association or organization, it is more secure than open cloud because of its impediments and confinements. It will work inside an association however can be overseen by the outsider. For hybrid, it is a mix of Public Cloud and Private Cloud, it is setting up a connection between open cloud and private cloud. Then based on service types, there are numerous subtleties of distributed cloud computing as an idea, but there are three main approaches that enterprises will take benefit of it. First Software as a Service (SaaS) which defines as complete product is run and overseen by the specialist service provider and conveyed by means of the web. These are regularly the applications could use by customers throughout each and every day. Second Platform as a service (PaaS), for this situation, the Platform is supervised by a specialist organization while developers can build and oversee applications within the environment. Third Infrastructure as a service (IaaS), the least comprehensive type of cloud computing, IaaS offers the construction chunks of IT for business to govern. From networking features to data storage, IaaS gives you on-premises IT resources without the capital expenditure economic model. The certainty is that IT crews must be experienced in each type of cloud computing. The contemporary IT organization will comprise of a combination of each category. The market of cloud computing solutions and services continues to grow more crowded.

Cloud computing is a significant worldview, with the possibility to altogether diminish cost through enhancement and expanded working and monetary efficiencies. Besides, Cloud computing could fundamentally improve joint effort, agility and scale, in this way empowering genuinely worldwide figuring model over the internet infrastructure frameworks, where nobody should keep up their very own private data center units. Be that as it may, there is a tremendous assortment of hindrances before cloud computing can be widely deployed. An ongoing review by Oracle alluded the information source from international data corporation enterprise panel, demonstrating that security speaks to 87% of cloud clients' feelings of dread. One of the significant security worries of cloud clients is the assurance on data of their re-appropriated records since they never again physically have their information and accordingly lose the power over their information. Also, the cloud server isn't completely trusted and it isn't

required for the cloud server to report information misfortune occurrences. Thus, we have taken up this task with the worry of security in the cloud.

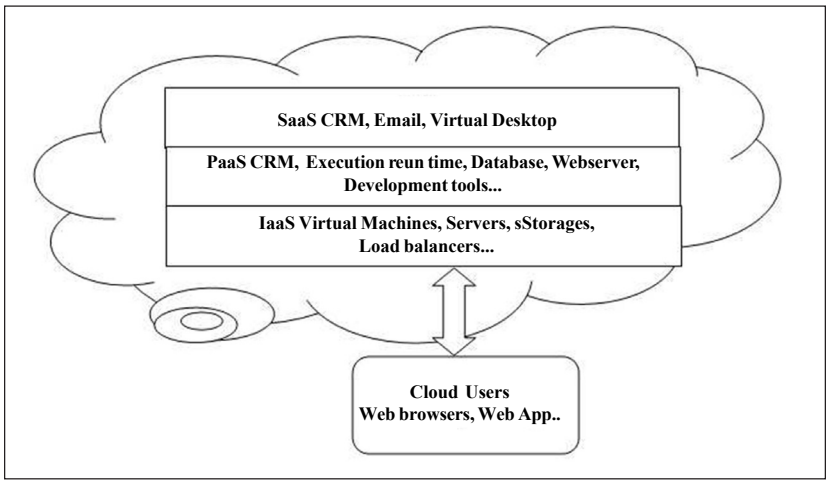

Figure 2. Cloud Services

2.1. Cloud Computing Security

Preceding cloud computing, users of cloud applications did not request the degree of security from service providers that they do today. Those saleable cloud applications were kept running inside the customer's edge behind the providers firewall. With Cloud condition, administration vendors have more prominent duties to verify the applications for the benefit of the client's. Since customers were surrendering control and frequently enabling their information to live outside of their firewall, they requesting that the service providers consent to different guidelines. This is the much needed development for those of us who have been waving the warning the previous quite a while about the absence of spotlight on application security in the endeavors. There is a typical legend that basic information in the cloud can't be secure. Actually security must be architected into the framework paying little mind to where the information lives. Cloud security alludes to a wide arrangement of approaches, innovations, and controls conveyed to ensure information, applications, and the related framework of cloud. It is a sub-area of computer security, network system security, and, all the more extensively, data security. [7]

Most applications worked in the cloud, public or private, are dispersed in nature. The reason numerous applications are manufactured like this is so they can be modified to scale on a level plane as interest goes up. An ordinary cloud design may have a dedicated web server farm, a database server farm, and a caching server farm. In expansion, each homestead might be repetitive over numerous data centers, physical or virtual. As one can envision, the quantity of servers in an adaptable cloud design can develop to an abnormal state. Cloud environment furnishes clients with abilities to store and process their information in third party data centers. Associations utilize the cloud in a wide range of administration models and arrangement models. Security concerns related with cloud environment fall into two general classes: security issues looked by cloud provider and security issues looked by their clients (companies or associations who host applications or store information on the cloud). The duty is shared, nonetheless. The provider must guarantee that their foundation is secure and that their customers' information and applications are ensured, while the client must take measures to strengthen their application and utilize solid passwords and confirmation measures. Fundamentally the providers ought to apply the accompanying three techniques for overseeing security in a cloud based application. As Like centralization, standardization and computerization. Centralization alludes to the act of merging a lot of security controls, processes, approaches and administrations and diminishing the quantity of spots where security should be overseen and actualized. In standardization security ought to be thought of as a core administration that can be shared over the undertakings, not an answer for a particular application. Each application having its own novel security solutions. In automation security highlights are consolidating naturally scale as demands increments or diminishes, virtual machines and code arrangements must be scripted so no human intercession is required to stay aware of interest.

2.2. Cloud Security Controls

Cloud security design is compelling just if the right guarded executions are set up. A productive cloud security engineering ought to perceive the issues that will emerge with security the board. The security management tends to these issues with security controls. These controls are set up to shield any shortcomings in the framework and decrease the impact of an assault. While

there are numerous kinds of controls behind a cloud security engineering, they can as a rule be found in one of the accompanying categories. Such as deterrent controls, preventive controls, detective controls and corrective controls. In deterrent controls are proposed to decrease assaults on a cloud framework. Much like a notice sign on a fence or a property, obstruction controls normally decrease the danger level by educating potential aggressors that there will be disapproving ramifications for them on the off chance that they continue. (Some think of them as a subset of preventive controls.)Preventive controls reinforce the framework against episodes, for the most part by lessening if not really disposing of vulnerabilities. Solid validation of cloud clients, for example, makes it more outlandish that unapproved clients can access cloud frameworks, and almost certain that cloud clients are decidedly recognized.

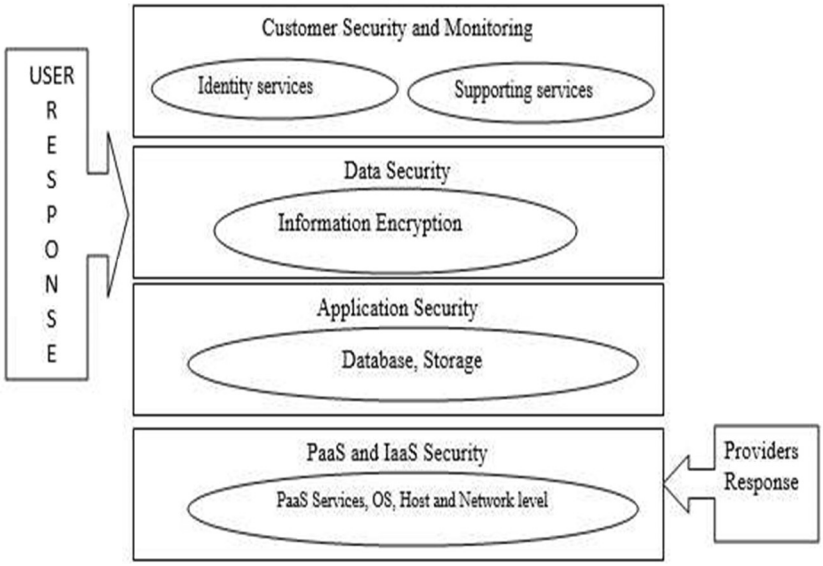

Figure 3. Cloud Security Architecture

Detective controls are planned to distinguish and respond fittingly to any episodes that happen. In case of an assault, an investigator control will flag the deterrent or remedial controls to address the issue. Framework and system security checking, including interruption discovery and aversion game plans, are commonly utilized to distinguish attacks on cloud frameworks and the supporting framework. In Corrective controls decrease the outcomes of an occurrence, regularly by restricting the harm. They become effective during or after an episode. Reestablishing framework reinforcements so as to reconstruct a compromised framework is a case of a remedial control.

2.3. Cloud Security and Data Security

There are numerous security issues in cloud as they facilitate resources management over web equally follows. [8]

2.3.1. Physical Security

Cloud specialist organizations physically secure the IT equipment (servers, switches, links and so on.) against unapproved get to, obstruction, theft, fires, floods and so forth and guarantee that fundamental supplies, (for example, power) are adequately hearty to limit the likelihood of interruption. This is ordinarily accomplished by serving cloud applications from 'world-class' (for example expertly indicated, planned, built, oversaw, checked and kept up) data centers.

2.3.2. Personal Security

Different data security concerns identifying with the IT and different experts related with cloud administrations are commonly dealt with through pre-, para-and post-work exercises, for example, security screening potential volunteers, security mindfulness and preparing programs, proactive.

2.3.3. Privacy

Suppliers guarantee that every single basic datum (Credit card numbers, for instance) are covered or encoded and that lone

approved clients approach information completely. Besides, advanced personalities and qualifications must be secured as should any information that the supplier gathers or delivers about client action in the cloud.

2.3.4. PKI Management

Each undertaking will have its very own PKI the executives' framework to control access to data and figuring assets. Cloud suppliers either coordinate the client's PKI the board framework into their own foundation, utilizing organization or SSO innovation, or a biometric-based ID framework, or give a PKI the board arrangement of their own.

2.3.5. Data Security

Various security issues are related with cloud data administrations: not just customary security issues, for example, network snooping, unlawful intrusion, and Denial reply in distributed environment, yet in addition explicit distributed computing threats, for example, side channel assaults, virtualization vulnerabilities, and maltreatment of cloud administrations. The accompanying security necessities limit the threats.

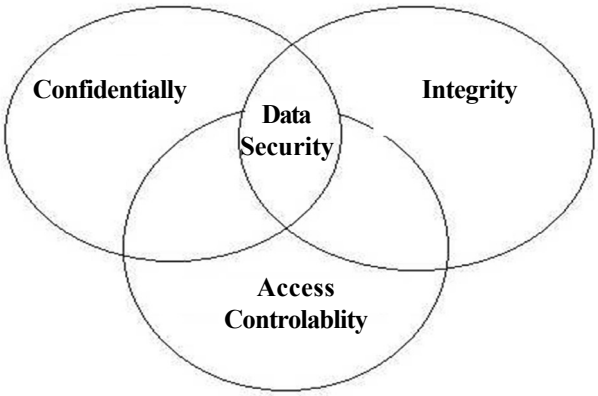

Figure 4. Data Security Confidentiality

Data confidentiality is the property that information substance are not made accessible or uncovered to unlawful clients. Redistributed information is put away in a cloud and out of the client's immediate control. Just approved clients can get to the delicate information while others, including TPAs, ought not to increase any data of the information. In the interim, information owners hope to completely use cloud information administrations, e.g. data search, information process, and information sharing, without the spillage of the information substance to TPAs or other challengers.

2.3.6. Access Controllability

This implies that an information owner can play out the particular limitation of access to her or his information re-appropriated to cloud. Legitimate clients can be approved by the owner to get to the information, while others can't get to it without consents. Further, it is alluring to implement fine-grained access control to the re-appropriated information, i.e., various clients ought to be allowed distinctive access benefits with respect to various information pieces. The access approval must be controlled distinctly by the owner in untrusted cloud conditions.

2.3.7. Integrity

Data integrity requests keeping up and guaranteeing the exactness and fulfillment of information. An information owner dependably expects that her or his information in a cloud can be put away accurately and reliably. It implies that the information ought not be unlawfully altered, inappropriately changed, intentionally erased, or maliciously manufactured. In the event that any bothersome tasks degenerate or erase the information, the data owner ought to have the option to identify the debasement or loss. Further, when a segment of the redistributed information is tainted or lost, it can at present be recovered by the data users.

3. Existing and Proposed Method

In existing framework [9], the data misfortune was obviously little in respect to the all-out data put away, yet any individual who runs a site can promptly see how unnerving a prospect any data misfortune is. Now and again it is deficient to recognize data defilement when getting to the information since it may be past the point where it is possible to recoup the tainted data.

Accordingly, it is vital for cloud clients to as often as possible check if their re-appropriated data are put away appropriately.The size of the cloud information is enormous, downloading the whole document to check the trustworthiness may be restrictive as far as data transfer capacity cost, and henceforth, illogical. Besides, conventional cryptographic natives for data integrity checking, for example, hash functions, approval code (MAC) can't make a difference here legitimately due to being short of a copy of the original file in verification. The current RDIC conventions experience the ill effects of the issue of a complex administration, that is, they depend on the public key infrastructure (PKI), which may ruin the deployment of RDIC in practice.

Proposed framework utilizes PKI-based RDIC protocol to diminish the system complexity in nature. It likewise gives zero knowledge security against an outsider verifier and releases no data of the put away information to the verifier during the RDIC procedure. The main thing is client needs to send their reviewing request to verifier. This framework utilizes DriveHq as cloud specialist provider which is the finest for storage. The target objective is to check data integrity in cloud utilizing public auditing, PKI based remote data integrity trustworthiness checking ideas. By this, the proposal can guarantee the accuracy of data in the cloud condition.

4. Literature Review on Data Integrity Approach

The literature study demonstrates that a wide range of methodologies for cloud data integrity checking utilizing auditing have been as of now actualized. Experts anticipated an issue just because that empowers data proprietors to check the integrity of remote data without unequivocal learning of the whole information. As of late, remote data integrity checking turns out to be increasingly noteworthy because of the advancement of distributed storage frameworks.

Ateniese [1] proposed method called as Provable data possession which is a freely obvious component which permits not just the Owner yet anybody to Challenge the Server all things considered Challenge-Response Algorithm and it uses the Homomorphic Properties. There has been numerous extemporization given dependent on this Mechanism and to help the developing Multi-Cloud Environment. But it give a correspondence cost of request $O(1)$. Considered dynamic PDP plot just because based on hash capacities and symmetric key encryptions, which means the data owner can powerfully refresh their file after they store their information on the cloud server. This plan is effective yet has just set number of inquiries and block insertion can't expressly be supported.

A. Juels [2] a model is proposed called as Proofs of retrievability which relies upon preprocessing the Data by the customer before sending the Data or Uploading it. A few Issues with Updating were defeated in Compact form however it can just enhance to Communication Cost O(t).

Kan Yang [3] a model is proposed called as Third-Party Storage Auditing Service which uses Data Fragment Technique and Homomorphic Verifiable Tags to decrease Communication Cost just as to improve Performance. The accompanying area gives the definite clarification on Data Trustworthiness Verification Schemes. The Major three methodologies of information Integrity that are incorporated as Provable data possession (PDP), Proofs of Retrievability (POR), and Third-Party Storage Auditing Service (TSAS). In PDP scheme [4], guaranteeing the integrity of the data when it is being redistributed to a third party as data storage service. It empowers the alternative of checking the Integrity of uploaded data without getting the entire stored data from the server which is helpful on the situation that there has been a huge data stored on the server. It was presented as a substitute for the conventional signature marks and Hash calculations. A Proof of retrievability is comparable plan to that of Provable data Possession, It gives the verification that a record is Intact and not changed by any assault [2]. This helps more in characterizing the presence of information than that of Integrity (i.e.) Helps more in Checking the full Existence of data .Hence it is gives the verification of Existence. They devour less data transfer capacity than the record itself and consequently can be utilized in remote condition. The fundamental component that happens in this Scheme is that they can right any Data Corruptions that is found by utilizing Error Revision codes.

This Scheme [3] is additionally utilized for checking data integrity in the cloud Environment. The property utilized in this component is Bilinearity Property. This Property is utilized to make a proof framework that is scrambled alongside a stamp that helps the information proprietor to challenge the Cloud Server. Thus Data Privacy is overseen so that a Third Party Auditor can't decode the message while reviewing. Likewise it doesn't require any Organizer while doing examining on Multi-Cloud condition. Also This Scheme empowers the server to check the worth some of the time so that can be utilized by Auditor subsequently diminishing the heap on the Auditor itself consequently burden adjusting is accomplished so more effectiveness is

accomplished. R. Burns [5] considered dynamic PDP conspire just because based on hash capacities and symmetric key encryptions, which means the data owner can powerfully refresh their document after they store their information on the cloud server. This plan is proficient yet has just set number of inquiries and square inclusion can't expressly be bolstered. Q. Wang [6] proposed the idea of "zero-learning open reviewing" to oppose disconnected speculating attack. Be that as it may, a formal security model isn't given in this work. The first ID-based PDP was proposed in which changed over the ID-based aggregate signature because of Gentry and Ramzan to an ID-based PDP protocol. Also proposed [6] another PKI-based provable information ownership in multi-distributed storage. Nonetheless, their security model for PKI-based PDP isn't sufficient for catching the property of soundness.

5. Methods

The proposed method to ensure data integrity with zero knowledge of verifier using PKI built RDIC mechanism.

In public cloud environment, users information been stored server which managed by cloud data center. Third party auditor has to monitor the data environment which owned by cloud provider. Key generation center authorized data owner based on login credential details. User can identified by PK which provided by key generation center. Data owner can ensure the data integrity through arising auditing request to TPA and auditing proof has to submit by service provider. This process get complete when auditing message received by provider and the same will shared to data owner in the form of report. In the intervening time if there is any intruders attack service provider environment that has to prevent by enquiring valid keys to ensure.

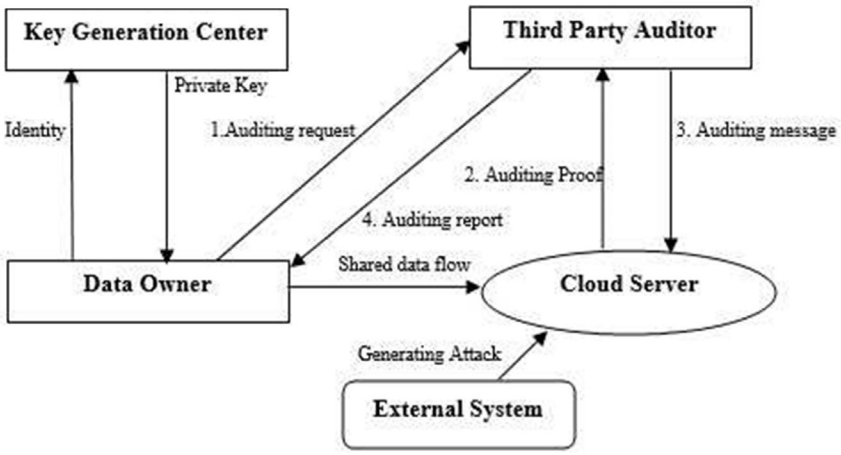

Figure 5. System Architecture

Table 1 contains the description of software framework that are required to setup the private cloud, deploy the web application over the cloud and how to use the client side application and ways to perform experimentation with user data.

Programming languages	Scripts	Data base	Online Cloud Provider
Java, JSP	HTML, CSS, Glass fish 3.1.2.2	MYSQL	DriveHq

Table 1. Software description

DriveHQ (Drive Headquarters Inc.) is a cloud IT specialist co-op for the most part in the endeavor service market. DriveHQ's highlights incorporate Cloud File Server, WebDAV Drive Mapping, Cloud Storage, Online Backup and FTP Server Hosting. DriveHQ was established in 2003. As of Mar. 2016, DriveHQ has over 2.5 million enrolled clients. Among the biggest customers are Fortune 500 organizations, for example, Disney, Orange, Alstom, Cummins, and so on. In 2012, DriveHQ propelled Cloud Recording and Surveillance administration CameraFTP.com.

Figure 6. DriveHq Login

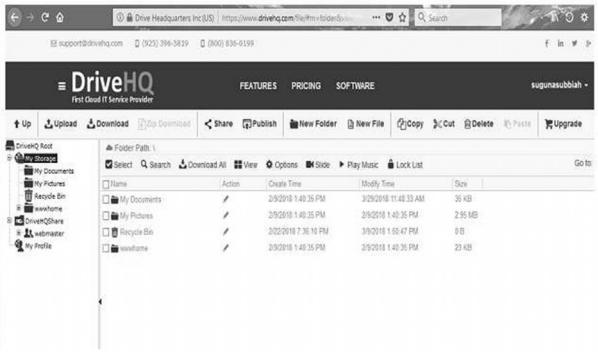

Figure 7. DriveHq desktop client

The proposed method comprises the sections are user interface, Key generation, File uploading Process, Attacks generator, user challenges, proof generation and final check.

The goal of User interface (UI) configuration is to create a UI which makes it simple (clear as crystal), effective, and easy to use to work a machine in the manner in which creates the ideal outcome. This for the most part implies that the administrator necessities to give negligible contribution to accomplish the ideal yield, and furthermore that the system limits undesired yields to the human. Our task gives proficient UI structures as login authentication and so on. The KGC (Key Generation Center) is a piece of a cryptosystem planned to decrease the risk characteristic in trading keys. KGCs frequently work in frameworks inside which a few clients may have authorization to utilize certain administrations at certain occasions and not at others. An ordinary task with a KGC includes a solicitation from a client to utilize some administration. The KGC will utilize cryptographic strategies to confirm mentioning clients as themselves. It will likewise check whether an individual client has the option to get to the administration mentioned. On the off chance that the validated client meets all endorsed conditions, the KGC can issue a ticket allowing access.

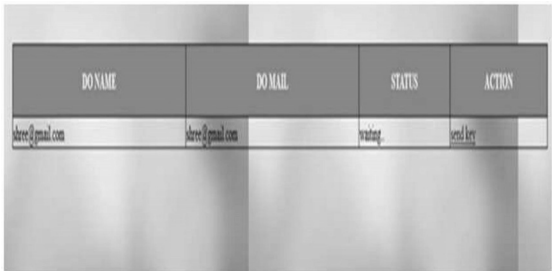

Figure 8. Key Generation Center

Figure 9. File Uploading

File uploading process includes DriveHq cloud server which we are utilizing to store the transferred information. Each client can make his/her very own record in DriveHq for their motivations. Client can transfer information from their nearby PC. At the point when client chooses the information from the nearby framework, they have to choose the document name, record way. Utilizing PKI component, client needs to encode the document utilizing private key and create hash code for the scrambled record. Subsequently, client needs to transfer the scrambled document to the cloud which serves security against the server. For guaranteeing information integrity, we have to show cloud attack to adjust the information put away in the cloud. For that reason, Phishing attack which is one of the cloud attack is utilized. Phishing is the endeavor to get sensitive data, for example, usernames, passwords, and credit card information, frequently for malicious reasons, by disguising as a dependable substance in an electronic correspondence. Phishing is normally completed by email mocking or texting, and it frequently guides clients to enter individual data at a phony site, the look and feel of which are indistinguishable from the real one and the main contrast is the URL of the site in worry .By utilizing attack, will get the confirmation certifications of DriveHq user (victim) and after that alter the document stored in the cloud.

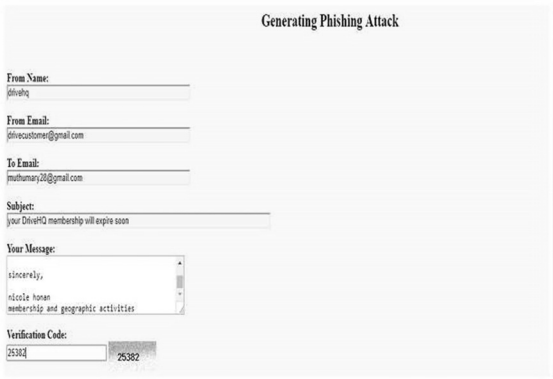

Figure 10. Generating Phishing Attack

Figure 11. TPA Audit Request

In user challenge, before the file to be transferred to the cloud, it must be scrambled utilizing client's private key and afterward hash value ought to be produced .After effective transferring of client's document, client may wish to guarantee the integrity of data. All things considered, client need to challenge the cloud server by means of TPA. Since the file is scrambled, the TPA ought to be ignorant of the document substance and hash code doesn't give any data about the record toTPA. In proof generation process involve with cloud server assumes a crucial job in proof generating process.After getting challenge from client, TPA will in general exchange the test solicitation to cloud for integrity checking purpose. TPA sends record id and file name to the cloud server. The cloud server finds the relating record utilizing filename. At that point, it creates the hashcode for the record which is just in encoded position .This gives security against malicious cloud server. Once the hash code is produced, cloud server sends the hashcode to TPA .The TPA performs integrity checking process. For proof check process involves when the TPA gets cloud server computed hashcode, it does following methods.

Case 1: The TPA likewise keeps up the client created hashcode. It analyzes the hashcode from client and hashcode from cloud

server. If the information isn't defiled by any external system, the returned value must be 1. That is, the information isn't ruined.

Case 2: Any external system, may ready to degenerate the client's data stored in cloud which is avail form of encoded format, there might be an opportunity to alter the encoded data. At the point when the information is modified, while TPA looks at the client's hashcode and cloud server's hashcode, the returned value must be 0.That is, the information is corrupted.

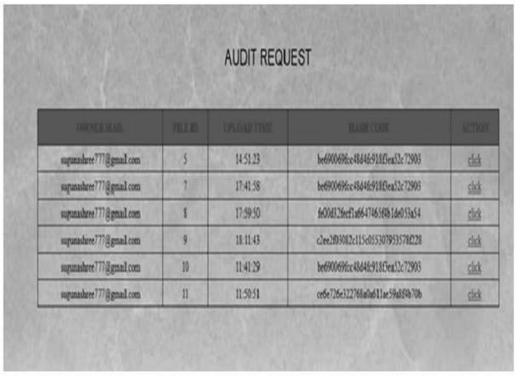

Figure 12. Data Owner Audit Request

Figure 13. Proof Verification

6. Conclusion

The cloud storage carries the helpful method to access files through various gadgets. In any case, one of the issues is security on the grounds that the file which is transferred could be stolen by unapproved people. Information security against the third party verifier is very basic since the cloud clients may store confidential or sensitive files to the cloud. Be that as it may, this issue has not been completely explored. The proposed PKI built RDIC framework guarantees correctness of information by giving protection from the malevolent server and accomplishes zero knowledge security against a verifier. The clients encode the document before transferring and the decoding key is recollected by the client itself thus it gives the protection from cloud server and furthermore TPA doesn't have direct access to client's data.

References

[1] Ateniese, G., Burns, R. C., Curtmola, R.J. Herring, L. Kissner,Z. N. J. Peterson, and D. X. Song, Provable data possession at untrusted stores, *In*: ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F.Syverson, Eds. ACM, 2007, p. 598–609.

[2] Juels, A., Jr, B. S. K. (2007). Pors: proofs of retrievability for large files, in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, p. 584–597.

[3] Kan Yang and XiaohuaJia., TSAS: Third-Party Storage Auditing Service, *In:* Security for Cloud Storage Systems,SpringerBriefs in Computer Science 2014, p 7-37.

[4] Venkat Rao, K., AvalaAtchyutaRao. (2013). Data Integrity in Multi Cloud Storage, *International Journal of Science Engineering and Advance Technology*, 1 (7) 2013.

[5] Ateniese, G., Di Pietro, R., Mancini, L. V., Tsudik, G. (2008). Scalable and efficient provable data possession, in Secure Comm '08: *In*: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York, NY, USA, 2008, p 1–10.

[6] Wang, Q., Wang, C., Li, J., Ren, K., Lou, W. (2009). Enabling public verifiability and data dynamics for storage security in cloud computing, *In:* ESORICS'09: Proceedings of the 14th European Conference on Research in Computer Security, Berlin, Heidelberg, 2009, 355–370.

[7] Cloud Security Alliance. (2010). Top Threats to Cloud Computing. [Online]. Available: http://www.cloudsecurityalliance.org

[8] Wang, C., Wang, Q., Ren, K., Lou, W. (2009). Ensuring data storage secruty in cloud computing, *In*: Proceedings IWQoS, 2009, p. 1–9.

[9] Zhu, Y., Hu, H., Ahn, G.-J., Yau, S. S. (2012). Efficient audit service outsourcing for data integrity in clouds, *J. Syst. Softw*., 85 (5) 1083–1095.

[10] Barsoum, Ayad F., Anwar Hasan, M. (2012). Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers. Proceedings of the 12th *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2012, p 829-834.

Author Biographies

V. Arulkumar, Assistant Professor of Information Technology has over 11 years of experience. His graduated in B.E Information Technology and post graduate in M.E Computer Science and Engineering. His area of interests are scheduling on cloud based services, provide security, trust and integrity on cloud data centers. Currently doing his research in cloud technologies on ensuring integrity for data sharing.

Dr. N. Bhalaji, Associate Professor of Information Technology has over 14 years of teaching experience. He received his B.E. & M.E. degree both in the discipline of Computer Science and Engineering and Ph.D. specializing in Trust Based Routing approach for MANET's from Anna University, Chennai. His current research interests are the Application of Trust over information and communication domains namely Internet of Things and exploring Machine learning algorithms to improve quality of social outlook.