INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

Enhanced Integrity Preserving Homomorphic Scheme for Cloud Storage

Mashkoor Ahmad Kichloo[1], Mr. Parikshit Singla[2]

Student[1], Assistant Professor[2]

Department Of Computer Science and Engineering, DVIET, Karnal

Haryana, Karnal-132001

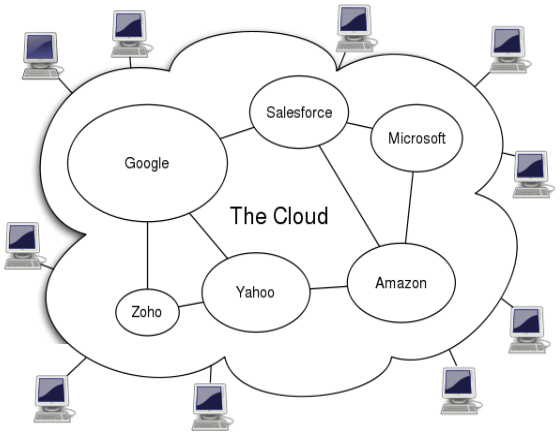
Abstract— As Cloud Calculating becomes prevalent, extra and extra sensitive data are being centralized into the cloud, such as emails, confidential condition records, confidential videos and photos, firm finance data, power documents, etc. By storing their data into the cloud, the data proprietors can be relieved from the burden of data storage and maintenance so as to relish the on-demand elevated quality data storage service. Though, the fact that data proprietors and cloud server are not in the alike trusted area could locale the our sourced data at chance, as the cloud server could no longer be fully trusted in such a cloud nature due to a number of reasons: the cloud server could leak data data to unauthorized entities or be hacked. It follows that sensitive data normally ought to be encrypted prior to outsourcing for data privacy and combating unsolicited accesses. In cloud computing cloud users and cloud ability providers are nearly precise to be from disparate belief domains. Data protection and privacy are the critical subjects for remote data storage. A safeguard user enforced data admission manipulation mechanism have to be endowed beforehand cloud users have the freedom to outsource sensitive data to the cloud for storage. With the rise of allocating confidential company data on cloud servers, it is imperative to accept an effectual encryption arrangement alongside a fine-grained admission manipulation to encrypt outsourced data. Attribute-based encryption is an area key established encryption that enables admission manipulation above encrypted data employing admission strategies and ascribed attributes. In this work, we are going to scutiny homomorphic schemes for encryption and probable resolutions for their limitations.

Keywords: Cloud Computing, Encryption, Homomorphic Schemes

I. INTRODUCTION

Cloud computing, as a producing computing paradigm aiming to allocate storage, computation, and services transparently amid a colossal users, has gathered outstanding momentum from not merely industry but additionally academia. In core, cloud computing [1] overlaps countless tolerating thoughts, such as distributed, grid and utility computing. Though, driven generally by marketing and skill offerings from colossal firm contestants like Google, IBM and Amazon, cloud computing has evolved out of these thoughts and come to be a new buzz word pondering on“ cloud”—more hypothetical resource and services’ delivery. Later cloud computing steps into our daily lifetimes, every single innately stored data, such as email, word processing documents and spreadsheets, could be remotely stored in a cloud. Then, we can use every single terminals, e.g., computer, laptop and PDA etc., to admission this data at anytime, anywhere. Due to these enthusing characteristics, cloud computing has come to be increasingly appealing to the public.

The "cloud" in cloud computing can be delineated as the set of hardware, webs, storage, services, and interfaces that link to grasp aspects of computing as a service[2][3]. Cloud services encompass the transport of multimedia, groundwork, and storage above the Internet instituted on user demand. Cloud computing has four vital characteristics: elasticity and the skill to scale up and down, self-service provisioning and automatic DE provisioning, appeal multimedia design interfaces (APIs), billing and metering of skill rehearse in a pay-as-you-go flawless Figure 1.1 below displays a normal cloud era on the web. This flexibility is what is appealing people and firms to move to the cloud. Pursuing are the insufficient gains of owning an appeal hosted on the cloud:



:

Figure 1: General architecture in cloud computing environment

- It is the best cost efficient method to maintain, use and also to upgrade.
- Cloud computing is more cheap and also reduces the company's expenditure. Here you can pay only for the cloud space you need.
- You can get the ultimate storage according to plans provided by the cloud provider.
- The cloud service provider who is responsible for IT assets and maintenance.
- It is easy to access information all over the world using internet connection .you can also store the documents to your office staff.
- It also decreases company's carbon discharge by 35%.

Cloud computing can completely change the method firms use vision to skill clients, partners, and suppliers. A slight firms, such as Google and Amazon, by nowadays have most of their IT resources in the cloud. They have discovered that it can remove countless of the convoluted constraints from the instituted computing nature, encompassing space, era, domination, and cost [4].

A facile example of cloud computing is Yahoo email, Gmail, or Hotmail etc. With the possible of internet connection one can onset dispatching emails. The server and email association multimedia is all on the cloud and is totally grasped by the cloud skill provider Yahoo, Google etc. The client gets to use the multimedia alone and relish the benefits. Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Every single solitary segment serves a disparate aim and propositions disparate produce for firms and people considering the globe.

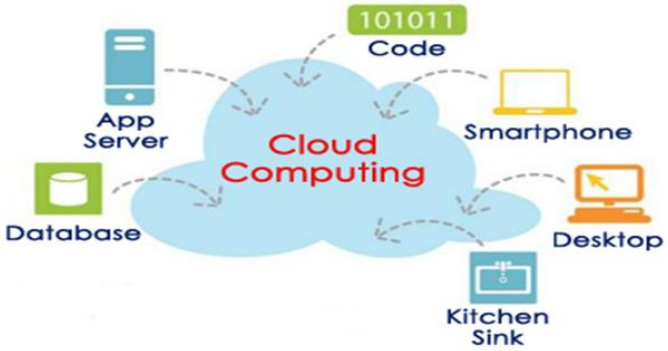


Figure 2: Cloud Platform on the web

II. ESSENTIAL CHARACTERISTICS:

1 On Demand Self-service:

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2 **Broad Network Access***:*

Capabilities are obtainable above the web and accessed across average mechanisms that advance use by heterogeneous slender or deep client periods (e.g. mobile phones, tablets, laptops, and workstations).

3 Resource pooling

The provider's computing resources are pooled to assist countless clients retaining a multi-tenant flawless, alongside disparate physical and adjacent resources vibrantly allocated and reassigned according to client demand. There is a sense of locale in dependence in that the

client normally has no manipulation or vision above the precise locale of the endowed resources but might be able to enumerate locale at a higher level of abstraction (e.g., state, state, or datacenter). Examples of resources encompass storage, processing, recollection, and web bandwidth [4].

4 Rapid elasticity:

Capabilities can be flexibly provisioned and released, in a little cases automatically, to scale quickly outward and inner commensurate alongside demand. To the customer, the skills obtainable for provisioning frequently materialize to be unlimited and can be seized in each number at each period.

5 Measured service:

Cloud arrangements automatically manipulation and optimize resource use by leveraging a metering capability1 at a slight level of abstraction appropriate to the kind of skill (e.g., storage, processing, bandwidth, and alert user accounts). Resource rehearse can be monitored, manipulated, and delineated, bestowing transparency for both the provider and client of the utilized skill.

III. SERVICE MODELS:

1 Software as a Service (SAAS):

The skill endowed to the client is to use the provider's demands running on a cloud infrastructure [5]. The demands are adjacent from varied client mechanisms across whichever a slender client interface, such as a web browser (e.g. web-based email), or a design interface. The client does not grasp or manipulation the underlying cloud groundwork encompassing web, servers, working arrangements, storage, or even individual appeal skills, alongside the probable exclusion of manipulated user specific appeal configuration settings.

2 Platform as a Service (PAAS):

The skill endowed to the client is to use onto the cloud groundwork consumer-created or acquired demands crafted retaining programming [6]. Normally this is finished on a pay-per-use or charge-per-use basis. A cloud groundwork is the collection of hardware and multimedia that enables the five vital characteristics of cloud computing. The cloud groundwork can be trusted as encompassing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are vital to prop the cloud services being endowed, and normally includes server, storage and web components. The abstraction layer consists of the multimedia utilized across the physical layer that manifests the vital cloud characteristics. Conceptually the abstraction layer sits above the physical layer, Languages, libraries, services, and instruments upheld by the provider.

The client does not grasp or manipulation the underlying cloud groundwork encompassing web, servers, working arrangements, or storage, but has manipulation above the utilized demands and perhaps configuration settings for the application-hosting nature.

3 Infrastructure as a Service (IAAS):

The skill endowed to the client is to skill processing, storage, webs, and supplementary frank computing resources whereas the client is able to use and run arbitrary multimedia that can encompass working arrangements and applications. The client does not grasp or manipulation the underlying cloud groundwork but has manipulation above working arrangements, storage, and utilized demands and perhaps manipulated manipulation of select networking constituents (e.g., host firewalls). The datacenter hardware and multimedia is what we will call a Cloud. Later a Cloud is made obtainable in a pay-as-you-go manner to the finished span, we call it a Expanse Cloud; the skill being vended is Utility Computing[7][8]. We use the word Confidential Cloud to denote to inner datacenters of a firm or supplementary association, not made obtainable to the finished span.

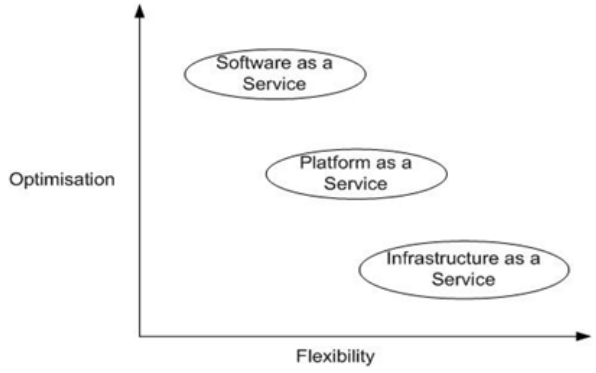


Figure 3 – Software, Platform and Infrastructure Services

IV. PRIVACY IN CLOUD COMPUTING

When a user stores a slight sensitive data in a cloud, the confidentiality of this sensitive data is of concern to the user. Lacking every single protection on this sensitive data, e.g., confidential business data, condition -records, a user won't have assurance in storing his/her sensitive data in cloud. Similarly, afterward a stable stores a slight firm documents, e.g., firm strategies, in a cloud, the stable additionally cares considering the confidentiality and hopes merely the relevant operatives can admission these documents afterward they are authorized. As well the confidentiality of these sensitive data, the user's individuality privacy, a frank right to privacy, is additionally anticipated in cloud computing. If the admission to a cloud discloses a user's real individuality, the user could yet be reluctant to accord this paradigm. Due to

this reason, the user authentication lacking knowing the real individuality, additionally yelled nameless authentication, is desirable in cloud computing. Even nevertheless nameless authentication can furnish user individuality privacy, it is a two-edged sword to furnish finished nameless admission in cloud computing. For example, afterward a cluster of users are authorized to a slight business computing or data-intensive logical collaborations in a cloud, if an vital data adjusted by someone is challenged, it is hard to trail the real user due to finished nameless authentication. Therefore, to tackle this dilemma, cloud computing must to additionally furnish provenance to record ownership and procedure past of data objects in cloud in order for expansive accord to the public. Safeguard provenance must to at least gratify the pursuing frank necessities:

- **Unforgeability**: a genuine provenance record in cloud computing can efficiently attest the ownership and procedure past of data objects stored in a cloud, each antagonist cannot forge a valid provenance records, i.e., modifying an item in a continuing record or undeviatingly familiarizing a new forged record lacking being noticed.
- **Conditional privacy preservation**: To safeguard data confidentiality and nameless authentication in cloud computing, a genuine provenance record must to additionally be conditional privacy maintaining That is, merely a trusted manipulation has the skill to expose the real individuality recorded in the provenance, as anybody else cannot.

Secure provenance is vital to the accomplishment of data forensics in cloud computing, yet it is yet a challenging subject today. Aiming at this, in this paper, we counsel a safeguard provenance scheme instituted on the bilinear pairing method to furnish trusted evidences for data forensics in cloud computing. Concretely, this paper will make the pursuing contributions:

- Firstly, the formal definition and security notions of secure provenance for cloud computing are introduced;
- Secondly, based on the bilinear pairings, a concrete secure provenance scheme is proposed, which can achieve the information confidentiality, anonymous access to the cloud, and conditional provenance tracking;

Thirdly, we use the provable security technique to validate its security in the standard model.

V. PROPOSED ALGORITHM

In counseled cryptosystem we find a supplementary property that there exists an effectual algorithm to compute an encryption of the sum or the product, of two memos given the span key and the encryptions of the memos but not the memos themselves. If M (message) is an additive (semi-)group, subsequent the scheme is yelled additive Otherwise, the scheme is yelled multiplicative. With respect to the aforementioned definitions, the pursuing points are worth noticing:

1. For a this encryption scheme to be efficient, it is crucial to make sure that the size of the cipher texts remains polynomial bounded in the security parameter σ during repeated computations.
2. The security aspects, definitions, and models of homomorphic cryptosystems are the same as those for other cryptosystems.

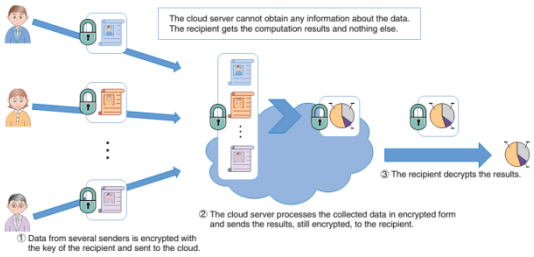


Fig: 4 Architecture for Proposed Model

VI. HOMOMORPHIC SCHEME FOR CLOUD INTEGRITY

When the data transferred to the Cloud we use average encryption methods to safeguard the procedures and the storage of the data. Our frank trusted was to encrypt the data beforehand dispatch it to the Cloud provider. But the last one needs to decrypt data at every single solitary operation. The client will demand to furnish the confidential key to the server (Cloud provider) to decrypt data beforehand present the calculations demanded, that might change the confidentiality and privacy of data stored in the Cloud.

we are counseling an appeal of a method to present procedures on encrypted data lacking decrypting them, that will furnish the comparable aftermath afterward calculations as if we have worked undeviatingly on the raw data. Homomorphic Encryption arrangements are utilized to present procedures on encrypted data lacking knowing the confidential key (without decryption); the client is the merely holder of the hidden key. Later we decrypt the consequence of every single procedure, it is the comparable as if we had grasped out the calculation on the raw data.

An encryption is homomorphic, if: from Enc (a) and Enc (b) it is possible to compute Enc (f (a, b)), where f can be: +, ×, ⊕ and without using the private key. Among the Homomorphic encryption we distinguish, according to the operations that allows to assess on raw data, the additive Homomorphic encryption (only additions of the raw data) is the cryptosystems, and the multiplicative Homomorphic encryption (only products on raw data) is the RSA and El Gamal cryptosystems.

- E k is an encryption algorithm with key k.

- Dk is a decryption algorithm.

$$D_k(E_k(n) \times (E_k(m)) = n \times m \; OR \; Enc\; (x \otimes y) = Enc(x) \otimes Enc(y)$$
$$D_L(E_L(n) \times (E_L(m)) = n \times m \; OR \; Enc\; (x \otimes y) = Enc(x) \otimes Enc(y)$$

The first property is called additive homomorphic encryption, and the second is multiplicative homomorphic encryption. An algorithm is fully homomorphic if both properties are satisfied simultaneously.

A. Multiplicative Homomorphic Encryption (RSA cryptosystem):

Let n = pq where p and q are primes. Pick a and b such that ab≡ 1 (mod ∅(n)). n and b are pubic while p. q and a are private.

$$e_k(x) = x^b mod\; n$$
$$e_k(y) = y^a mod\; n$$

The Homomorphism: Suppose x 1 and x 2 are plaintexts. Then,

$$e_k(X_1)e_k(X_2) = X_1^b X_2^b \; mod\; n = (X_1X_2)^b mod\; n = e_k(X_1X_2)$$

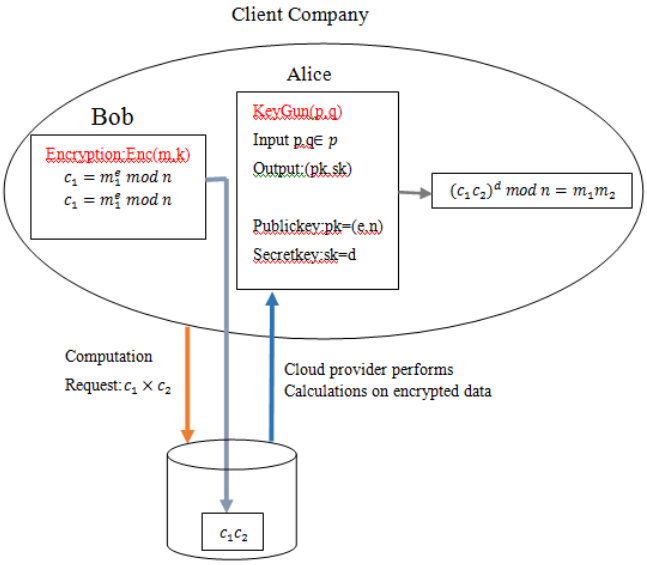


Figure 5: Multiplicative Homomorphic Encryption Applied to Cloud Computing

B. Additive Homomorphic Encryption:

Pick two largo primes p and q and lot n =pq. Let λ denote tho Carmichaol function, that is. λ (n)= Lcm(p – 1, q - 1). Pick random g ∈ $Z_{n^2}^*$ such that L(g^λ mod n^2) is invert**© modulo n (where L(u) =$\frac{u-1}{n}$). n and g are public; p and q (or λ) are private. For plaintext x and resulting ciphertext y. select a random r ∈ Z_n^*. Then

$$e_k(x,r) = g^x r^n mod\; n^2$$
$$d_k(y) = \frac{L(y^\lambda \; mod\; n^2)}{L(g^\lambda \; mod\; n^2)} mod\; n$$

To present supplement and multiplication on encrypted data stored in the cloud provider, the client have to have two disparate key dynamos (one for RSA and one for Paillier). We present in what follows the El Gamal cryptosystem that is basically a multiplicative homomorphic cryptosystem but by modifying coding mode we can make it additive.

C. El Gamal Cryptosystem:

Let p be a prime and pick $\propto \in Z_\rho^*$ such that n is a generator of Z_ρ^* Pick a and β such that $\beta \equiv \alpha^a$(mod p). $\rho, \propto, \beta \; are$ and are public; a is private. Let r ∈ Z_{p-1} be a secret random number. Then.

$$e_k(x,r) = (\propto^r \; mod\; \rho, x\; \beta^r mod\; \rho$$

El Gamal Cryptosystem performs multiplicative homomorphic encryption propriety:? Let x 1 and x 2 be plaintexts. Then

$$e_k(x_1,r_1)e_k(x_2,r_2) = (\propto^{r1} \; mod\; p, x_1\beta^{r1} mod\; p).(\propto^{r2} \; mod\; p, x_2\beta^{r2} mod\; p)$$
$$= \propto^{r1+r2} \; mod\; p, (x_1 + x_2)\beta^{r1+r2} mod\; p$$
$$= e_k(x_1x_2, r_1r_2)$$

If we put the plaintext in the exponent, we get:

$$e_k(x,r) = (\propto^r \; mod\; p, \propto^r \; \beta^r mod\; p)$$

Then the homomorphism is additive:

$$e_k(x_1, r_1)e_k(x_2, r_2) = (\propto^{r1} mod\ p, \propto^{x1} \beta^{x1} mod\ p)(\propto^{r2} mod\ p, \propto^{x2} \beta^{x1} mod\ p)$$
$$= (\propto^{r1+r2} mod\ p, \propto^{x1+x2} \beta^{r1+r2}) mod\ p$$
$$e_k(x_1 + x_2, r_{1+} r_2)$$

D. Fully Homomorphic Encryption:

For all kinds of calculation on the data stored in the cloud, we have to opt for the fully Homomorphic encryption that is able to present all kinds of procedures on encrypted data lacking decryption. In 2009 Craig Gentry of IBM has counseled the main encryption arrangement "fully homomorphic" that evaluates an arbitrary number of supplements and multiplications and subsequently compute every single solitary kind of aim on encrypted data. The appeal of fully Homomorphic encryption is an vital stone in Cloud Calculating security; supplementary normally, we might outsource the calculations on confidential data to the Cloud server, keeping the hidden key that can decrypt the consequence of calculation.

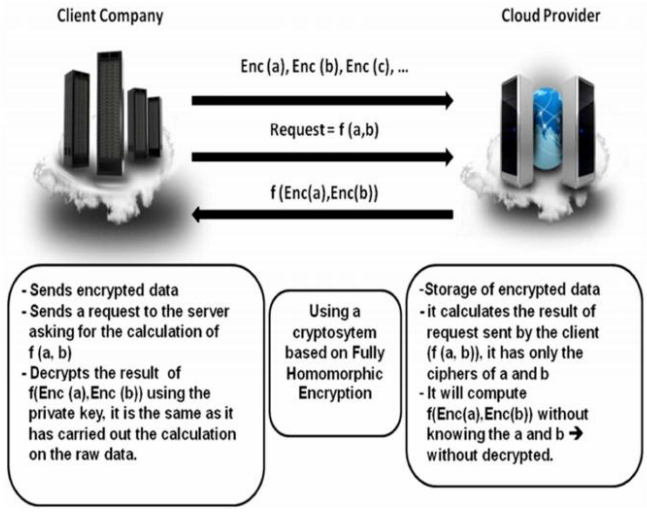


Figure 6. Fully Homomorphic Encryption applied to the Cloud Computing

VII. ALGORITHM STEPS

Consider a scenario in that a client has a slight sensitive data to procedure but needs the demanded expertise or adequate computational power; as a consequence, they desire to commission a cloud skill to grasp out the processing, but lacking revealing this sensitive data in plaintext form. The counseled encryption propositions a facile resolution to that problem; the client plainly sends the data to the cloud server in encrypted form, and the server procedures the data lacking decrypting it retaining the property of the counseled encryption (this computation on encrypted data is yelled homomorphic evaluation of the corresponding function). Finally, the client receives the encrypted output from the server and decrypts it alongside his key, obtaining the consequence of the processing lacking owning exposed every single data considering the sensitive data.

1. In first step, Cloud User Encrypts the Data and forwards it to Cloud Server.
2. The Cloud Server Computes the decryption keys on behalf of Cloud user so it knows what to look for with only Encrypted Message (no keys), It decrypts Cloud User data (perhaps only record by record, not all at once)/
3. The Server performs the requested or search/operations using the decrypted records of data.
4. The Cloud Server encrypts the requested results, if there are any, and return them back to Cloud User.
5. Additionally, Cloud User requires that, Cloud Server removes get rid of all remnants of computed key and decrypted records of data, on disk and in memory, data once the search is complete.
6. The Trused Party (Cloud Server) don't take advantage of Cloud User, since it is decrypting Cloud User data for this requests, to sneak in other searches at the same time, whether for my own benefit, or for one of Cloud User competitors.

The following diagram shows the sequence of the messages for a typical client/server session.

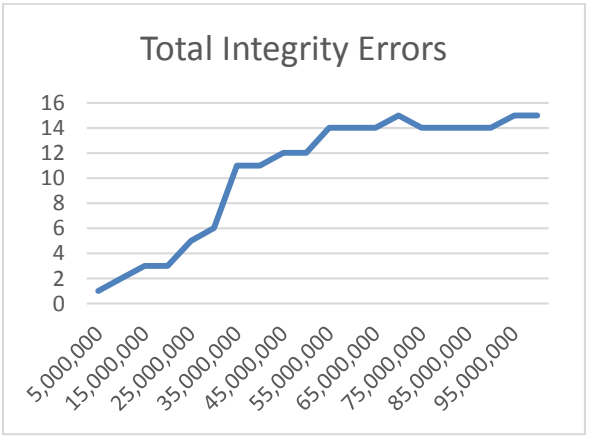


Fig: 7Total Integrity errors given the iterations

It is clear from above chart and table that out proposed integrity scheme produces minimum errors on average less than **1 error per Million Client Requests.**

10000 Iterations	20000 Iterations	30000 Iterations	40000 Iterations
11904946	19589798	30251343	40912888
12810879	21456636	28190187	34923738
11394205	21089223	28773522	36457821
12909182	19055739	29145317	39234895
14417366	19105216	29394454	39683692
16351427	20680839	28208511	35736183
17557635	21177097	27972217	34767337
12775411	21858291	28519641	35180991
17141168	22141427	30349116	38556805
19871818	24058961	31432040	39805119

Table: 1Total Running time for Cloud KeyGen and Checking Integrity Proofs

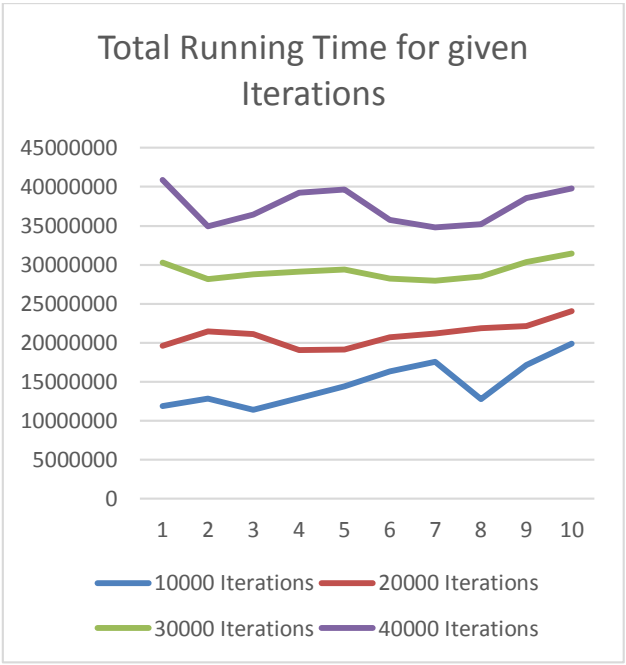


Fig: 8 Line chart showing total Running time for Cloud KeyGen and Checking Integrity Proofs, Indicates that the algorithm is linearly scalable

VIII. CONCLUSION

In this work, we have provided the design and implementation of Homographic scheme for verifying the integrity of multi-tenant cloud infrastructures. We have worked to enable the client in becoming a facts of integrity of the data that he wishes to store in the cloud storage

servers alongside bare minimum benefits and efforts. Our scheme was industrialized to cut the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server. Our Scheme produces minimum errors on average less than 1 error every single Million Appeal.

In cloud, there are countless gains to relief the burden of data association for users, such as facile to admission, inexpensive storage space, and convenient resource-sharing. Later users ponder their own manipulated storage space, they yearn to relish the convenient large storage space skill in cloud. Users normally upload data to the cloud storage servers, subsequent delete the innate copies. So users capitulated finished manipulation above the data itself. We counsel a safeguard data integrity checking decentralized erasure plan cloud storage arrangement instituted on the Elative allocate scheme. Our storage arrangement that consists of storage servers and key servers can completely halt malicious servers from ravaging our data that are partly decrypted. The counseled scheme can pledge confidentiality of memos for a long period of time. We have utilized a homomorphic encryption scheme that permits rising plaintext hidden inside of cipher texts and afterward retaining the homomorphic property joined alongside endeavored and tested "threshold cryptosystem", if in order to decrypt an encrypted memo, countless parties (more than a slight threshold number) have to cooperate in the decryption.

In this work, we have provided the design and implementation of Homographic scheme for verifying the integrity of multi-tenant cloud infrastructures. We have worked to enable the client in becoming a facts of integrity of the data that he wishes to store in the cloud storage servers alongside bare minimum benefits and efforts. Our scheme was industrialized to cut the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server. Our Scheme produces minimum errors on average less than 1 error every single Million Appeal.

IX. REFERENCES

1. Yubin Yang; Hui Lin; Jixi Jiang,"Cloud analysis by modeling the integration of heterogeneous satellite data and imaging",IEEE,Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 2006
2. Kaewpuang, R.; Uthayopas, P.; Srimool, G.; Pichitlamkhen, J.,"Building a Service Oriented Cloud Computing Infrastructure Using Microsoft CCR/DSS System",IEEE,Computer Sciences and Convergence Information Technology, 2009. ICCIT '09. Fourth International Conference on, 2009
3. Tao Wu; Kun Qin,"Inducing Uncertain Decision Tree via Cloud Model",IEEE,Semantics, Knowledge and Grid, 2009. SKG 2009. Fifth International Conference on, 2009
4. Yi Zhao; WenlongHuang,"Adaptive Distributed Load Balancing Algorithm Based on Live Migration of Virtual Machines in Cloud",IEEE,INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on, 2009
5. Zhifeng Xiao, Yang Xiao, "Security and Privacy in Cloud Computing", Dept. of Comput. Sci., Univ. of Alabama, Tuscaloosa, AL, USA, 10.1109/SURV.2012.060912.00182, 843-859, 2013
6. Schiffman, J., Yuqiong Sun, Vijayakumar, H., Jaeger, T., "Cloud Verifier: Verifiable Auditing Service for IaaS Clouds", , 10.1109/SERVICES.2013.37, 239-246, 2013
7. Meetei, M.Z., "Cloud computing and security measure", Dept. of Math., Jazan Univ., Jazan, Saudi Arabia, 10.1109/CISP.2013.6745284, 852-857, 2013
8. Pitropakis, N., Darra, E., Vrakas, N., Lambrinoudakis, C., "It's All in the Cloud: Reviewing Cloud Security", Dept. of Digital Syst., Univ. of Piraeus, Piraeus, Greece, 10.1109/UIC-ATC.2013.13, 355-362, 2013
9. Alabool, H.M., Mahmood, A.K., "Common Trust Criteria for IaaS cloud evaluation and selection", Dept. Comput. & Inf. Sci., Univ. Teknol. Petronas, Tronoh, Malaysia, 10.1109/ICCOINS.2014.6868444, 1-6, 2014
10. Hazarika, P., Baliga, V., Tolety, S., "The mobile-cloud computing (MCC) roadblocks", Siemens Technol. & Services, Bangalore, India, 10.1109/WOCN.2014.6923101, 1-5, 2014
11. Selvakumar, C., Rathanam, G.J., Sumalatha, M.R., "PDDS - Improving cloud data storage security using data partitioning technique", Dept. of Inf. Technol., Anna Univ., Chennai, India, 10.1109/IAdCC.2013.6506806, 7-11, 2013
12. Yongzhi Wang, Jinpeng Wei, Srivatsa, M., YucongDuan, Wencai Du, "IntegrityMR: Integrity assurance framework for big data analytics and management applications", Florida Int. Univ., Miami, FL, USA, 10.1109/BigData.2013.6691780, 33-40, 2013
13. Gibson, J., Rondeau, R., Eveleigh, D., Qing Tan, "Benefits and challenges of three cloud computing service models", Athabasca Univ., Athabasca, AB, Canada, 10.1109/CASoN.2012.6412402, 198-205, 2012