IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Enhancing Portability and Confidentiality of Data Migration Among Inter Clouds

[1]Gagandeep Kaur, [2]Kiranbir Kaur

[1,2]Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India

*Corresponding Author:deepsandhu2812@gmail.com

Available online at: www.ijcseonline.org

Accepted: 13/Aug/2018, Published: 31/Aug/2018

Abstract- Transferring information over the network is widely used fast and reliable source for communication. Users with wide fidelity use this mechanism for transferring and accessing information. Portability and interoperability within the cloud system through offline and online mediums are continuously desirable but the problem of security arises during the transmission process. Security and reliability is the key issue during the transfer process which is considered in this research. Information security is provided using the public and private key RSA cryptography. The experiment is implied not only at offline data but also at online data such as Google Docs. Redundancy handling mechanism is used to ensure that space at data storage provider is least used since cost in DSP is accompanied by the amount of storage used. Overall space requirement in case of heavy files is reduced and security of online information accessing is enhanced by the use of RSA cryptography with redundancy handling mechanism.

Keywords- Interoperability, Portability, Security, reliability, RSA, Redundancy, Cost

I. INTRODUCTION

The information security is a prime area of concern since vital information may be at stakes due to security problems in the transfer process or medium which is followed[1]. In order to tackle the issue, several strategies are in place. Every strategy works towards generating keys associated with the presented data. The redundancy of data given to the encryption process leads to the generation of multiple keys for similar data[2]. Also, the generated keys and data are stored at data and key storage providers. Storage of data and keys at storage providers require cost[3]. Size of the keys and data are directly proportional to cost. Resource provisioning within a federated cloud must consider reliability metrics as availability may or may not always enhances performance. Resources provided through VMs may be of no use in case VM fails. In order to address this issue VM migration, replication and fault tolerant protocol in the high-performance cloud. Cloud with a single provider is handled with the fault tolerance strategies but least amount of work is done towards the reliability aspect within federated cloud to this end disaster management, must be incorporated within the federation of cloud to enhance the execution if there should arise an occurrence of dynamic provisioning of resources from various cloud service organizations. Before describing details of techniques used to ensure security, cloud and its attributes are described as under.

Cloud Computing is a buzzword of 2010 and many experts disagree on its exact definition [4]. But the most used one and concurred one includes the notion of web-based services which are available on demand from an optimized and highly scalable service provider. Since such a disagreement on the definition, one will be provided for a better understanding of the notion. The cloud is IT as a service, delivered by IT resources that are independent of location. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet where end-users have no knowledge of, expertise in, or control over the technology infrastructure (the cloud) that supports them [5].

Cloud interoperability is required during the transmission of data to and from the cloud servers. The cloud service provides ensures QoS(quality of service) through security mechanisms. The security mechanisms used may or may not use redundancy handling mechanism to conserve space. In the proposed system security mechanism along with the redundancy handling mechanism is enforced for ensuring a quality of service. The attributes considered for evaluation are described as under.

1.1 ATTRIBUTES

Before some of the attributes will be defined, the term cloud should be explained. A cloud has been long used in IT, in network diagrams respectively, to represent a sort of black box where the interfaces are well known but the internal routing and processing is not visible to the network users[6]. Key attributes in cloud computing:

- **Service-Based*:*** Consumer concerns are abstracted from provider concerns through service interfaces that are well-defined.

- **Scalable and Elastic*:*** The service can scale capacity up or down as the consumer demands at the speed of full automation (from seconds for some services to hours for others) [7]. Elasticity is a trait of shared pools of resources. Scalability is a feature of the underlying infrastructure and software platforms.

- **Shared:**[8] Services share a pool of resources to build economies of scale and IT resources are used with maximum efficiency. The underlying infrastructure, software or platforms are shared among the consumers of the service (usually unknown to the consumers).

- **Metered by Use**: Services are tracked with usage metrics to enable multiple payment models[9]. The service provider has a usage accounting model for measuring the use of the services, which could then be used to create different pricing plans and models. These may include pay-as-you-go plans, subscriptions, fixed plans and even free plans.

- **Uses Internet Technologies**: The service is delivered using Internet identifiers, formats and protocols, such as URLs, HTTP, IP and representational state transfer Web-oriented architecture[10].
  The Encryption techniques collaborated with cloud computing to ensure a high degree of security and reliability is a prime objective of this study. File, as uploaded over the cloud, can be accessible to users of the cloud. Problems with the cloud are the malicious access as and when desired by users. Preventing the unauthorized access is the objective along with secure storage within the cloud. The contribution of this paper is listed as under
  • Describing key idea of security within the cloud system for secure storage and accessing of data
  • Applying security mechanism to be implemented on the online documents such as google docs.
  • Hybridizing RSA and DES for data encryption
  • Handling large data files and processing it with least amount of time.

II. RELATED WORK

[11] Describes IBE technique with outsourcing computation and also offloads the key generation operations to Key Update Cloud service provider. It also focuses on critical issues of identity revocation. It accomplishes consistent productivity for both calculation at PKG and private key size at client, User needs not to contact with PKG amid key-update, as it were, PKG is permitted to be disconnected subsequent to sending the disavowal rundown to KU-CSP, No protected channel or client verification is required amid key-update amongst client and KU-CSP.

[12] proposed the main mCL-PKE scheme without blending operations and gave its formal security. Our mCL-PKE takes care of the key escrow issue and disavowal issue. Utilizing the mCL-PKE conspire as a key building block, it proposed an enhanced way to deal with safely share sensitive information out in the public clouds. This approach support quick denial and guarantees the classification of the information put away in an untrusted open cloud while authorizing the entrance control strategies of the information proprietor. The exploratory outcomes demonstrate the productivity of fundamental mCL-PKE scheme and enhanced approach for people in general cloud. Further, for various clients fulfilling a similar access control arrangements, the enhanced approach performs just a solitary encryption of every datum thing and lessens the general overhead at the information owner. [13] Proposed a variation of CP-ABE to effectively share the various hierarchical documents in distributed computing. The hierarchical documents are scrambled with an incorporated access structure and the cipher text parts identified with characteristics could be shared by the records. Thus both cipher text storage and time cost of encryption is saved. The proposed system has benefits that clients can decode all approval documents by figuring secret key once. Therefore, the time cost of decryption is also saved if the client needs to decode various documents. Additionally, the proposed plot is ended up being secure under DBDH suspicion. [14] design a virtual encryption card framework that gives encryption card usefulness in virtual machines. In this framework, it displayed the vEC-PPM, which deals with the encryption resource plan. It saved clients' information utilizing a trusted equipment of virtualization in view of TPM. It additionally settled a trusted chain amongst clients and encryption cards in light of the composed protocols. The design of the virtual encryption card empowers the security and productivity of the encryption benefit. A usage examination shows that the effectiveness of framework is similar to that of the native mode. Later on, it proceed with examination, trying to plan a virtual encryption cards bunch to help higher encryption speed and more reasonable similarity with virtualization. [15] proposed a safe billing protocol for smart applications in distributed computing. It utilized homomorphic encryption through adjusting the Domingo-Ferrer's plan, which can perform different number arithmetic operations to fulfil smart grid billing necessities in a safe way. This plan keeps up the exchange off amongst security and versatility contrasted and other homomorphic plans that depend on either secure, yet inelastic in terms of arithmetic operations assortment. Additionally, it proposed an instrument that guarantees both security and integrity during correspondence between substances. The execution of the proposed system is very satisfactory; it is sufficiently productive to use in lightweight applications and can be helpfully connected to cloud-based applications. [16] propose a CP-ABE scheme that gives outsourcing key-

issuing, decryption and keyword search work. This scheme is productive since it just needs to download the fractional decryption cipher text relating to a particular keyword. In this scheme, the tedious matching operation can be outsourced to the cloud specialist organization, while the slight operations should be possible by clients. In this way, the calculation cost at the two clients and trusted specialist sides is limited. Besides, the proposed plot supports the capacity of keywords look which can enormously enhance correspondence effectiveness and further ensure the security and protection of clients. It is difficult to stretch out given KSF-OABE plan to help get to structure represent by tree in. [17]In this paper, based on contingent intermediary communicate re-encryption technology, an encrypted information sharing plan for secure distributed storage is proposed. The plan not just accomplishes communicate information sharing by exploiting communicate encryption, yet in addition accomplishes dynamic sharing that enables adding a client to and expelling a client from sharing gatherings dynamically without the need to change encryption open keys. Besides, by utilizing intermediary re-encryption innovation, this scheme empowers the intermediary (cloud server) to specifically share encoded information to the objective clients without the intercession of information owner while keeping information security, so significantly enhances the sharing execution. In the meantime, the rightness and the security are demonstrated; the execution is broke down, and the test comes about are appeared to confirm the possibility and the productivity of the proposed plot. [18]proposed diagram encryption scheme just makes utilization of lightweight cryptographic natives, for example, pseudo-arbitrary capacity and symmetric-key encryption, instead of moderate homomorphic encryptions. Accordingly, the proposed graph encryption scheme is well disposed to a wide arrangement of graph information based distributed computing and edge registering applications, for example, interpersonal organizations, e-maps, criminal investigations, and so on. Contrast with graph anonymization comes nearer from database group, proposed system achieves higher security level as the chart itself is encoded and it don't make any suspicions on the sorts of attacks. [19] reviewed a number of symmetric, public key and homomorphic cryptosystems to help practitioners understand encryption schemes for data on cloud storage. AES is used in most secure applications for data on cloud storage. Fully homomorphic encryption schemes are promising for cloud environment but are far from being practical because of their performance. Homomorphic evaluation of AES has interesting applications as a practical encryption scheme for data on cloud storage.

[20]proposed an Improved Encryption Calculation (EEA) for securing the data in cloud stockpiling. This is a symmetric encryption calculation. It utilizes same key for encoding and unscrambling the data previously put away in to cloud.[21]proposed a lightweight accessible open key encryption (LSPE) conspire with semantic security for CWSNs. LSPE decreases countless calculation escalated operations that are received in past works; along these lines, LSPE has seek execution near that of some useful accessible symmetric encryption schemes.[22] proposed a protected cloud data encryption framework, named the Circulated Ecological Key (DENK in short), with which all records are encoded by one encryption key got from numerous coordinating keys which are keys gotten from approved clients' secret key keys and a believed PC's natural key.[23] proposed to present an effective and unquestionable FHE in light of another mathematic structure that is without commotion.

[24] described various way which are used in cloud computing for data security. The information is put away on to incorporated area called data centres having a substantial size of information storage. In this way, the customers need to put stock in the supplier on the accessibility and additionally information security. Before moving information into general society cloud, issues of security gauges and similarity must be tended to. A trusted screen introduced at the cloud server that can screen or review the operations of the cloud server. In limiting potential security trust issues and additionally sticking to administration issues confronting Cloud computing, an essential control measure is to guarantee that a solid Cloud computing Service Level Agreement (SLA) is set up and kept up when managing outsourced cloud service suppliers and particular cloud merchants. Cloud computing guarantees to change the financial matters of the server farm, yet before sensing and managed information move.

To resolve the problem with the existing literature proposed literature present efficient solution. The encryption mechanism with the redundancy handling mechanism is proposed as described in the next section.

III. METHODOLOGY

The methodology of the proposed work consists of the registration process at first place. The registration in the proposed system will be a two-phase process. In the first phase, registration at data storage provider is made. After successfully registering, a user can load files at data storage provider end. To generate keys users require performing registration at a key service provider. In order to retrieve the files, users must login to the DSP and then KSP. The keys generated could be used in order to decrypt the file. The mechanism also uses redundancy handling mechanism for preserving space for extra file loading.

Also, online source of files like Google docs can be used to retrieve the files and perform encryption and decryption.

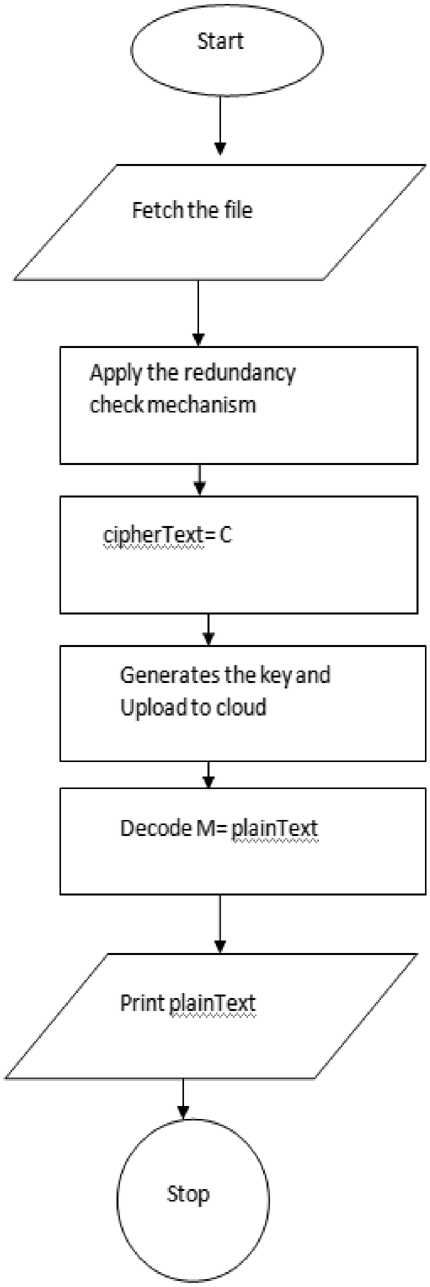
The detailed steps are described as under.

3.1 Registration at DSP

The registration at DSP comprises of unique username and password. Username and password once registered at DSP can be used for accessing the file uploading module.

3.2 Registration at KSP

A Key service provider(KSP) is used in order to generate the keys for the file which is uploaded. The proposed system is capable of generating the keys for files generated from online source.


Start
Fetch the file
Apply the redundancy check mechanism
cipherText= C
Generates the key and Upload to cloud
Decode M= plainText
Print plainText
Stop

3.3 Generating Keys

In order to generate keys, a user must login to the KSP. The files uploaded, are encrypted and corresponding keys are generated. The redundant files are neglected and rests of the files are uploaded with the public and private keys generated.

3.4 Encryption and Decryption

For encryption and decryption, AES and RSA algorithms are hybridized. The algorithm yield ciphertext after receiving files as plaintext. Verification of the overall procedure is in terms of time consumed and size of the file that can be uploaded.

IV. RESULT AND PERFORMANCE ANALYSIS

The result is presented in terms of file size that can be uploaded. Reliability of encryption and decryption in terms of time consumed is also a performance metric. The comparison in terms of quality is given as under

Table 1: Permitted Space Comparison

Performance Metric	File Size permitted Existing(KB)	File Size Proposed(KB)
Offline Source	20	50
Offline Source	22	57
Offline Source	50	102
Offline Source	65	165
Offline Source	85	200
Online Source	0	1024
Online Source	0	2048
Online Source	0	3000
Online Source	0	3987

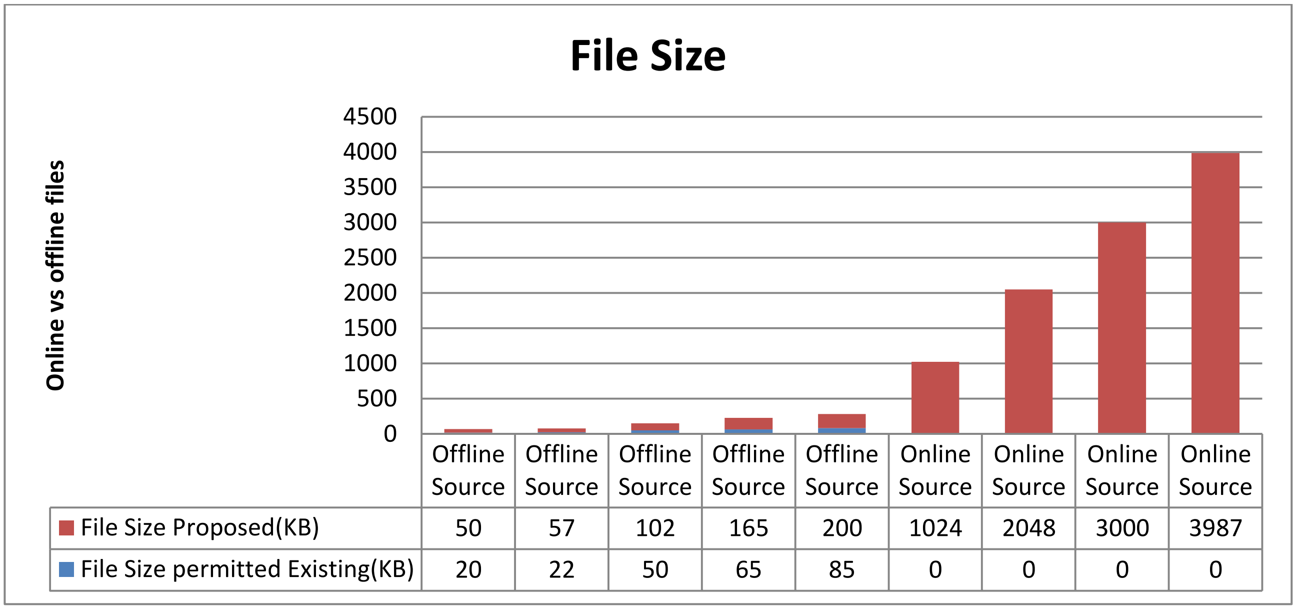


Figure 1: Plot of Space utilization by existing and proposed system

The time consumed also is an issue which can be further improved since time consumed greatly depends upon the speed of the internet used to access files from online source.

Table 2: Time Consumption Comparison

Source	File Size(KB)	Time Consumed Existing(ms)	Time consumed proposed(ms)
Offline	20	12	10
Offline	22	15	11
Offline	50	21	19
Offline	65	25	25
Offline	85	29	28
Online	1024	--	40
Online	2048	--	88
Online	3000		100
Online	3987		176

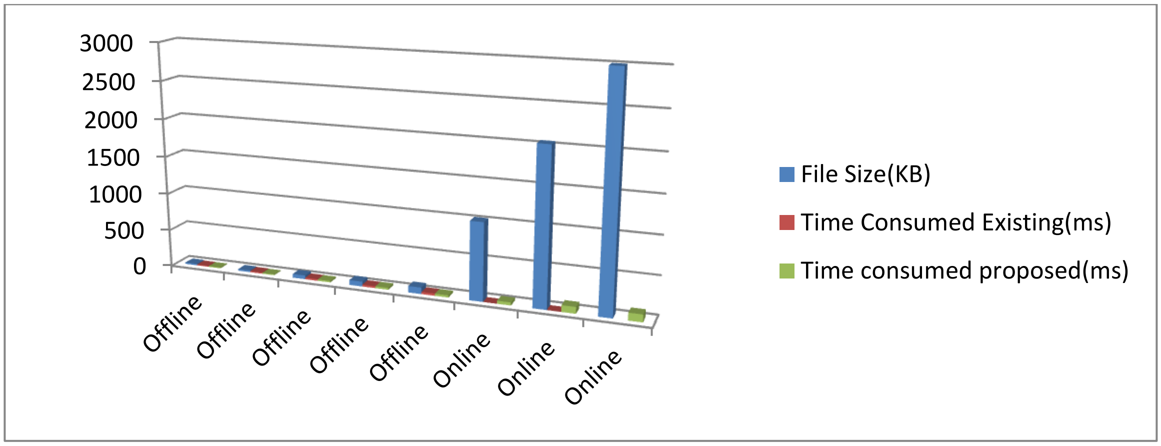


Figure 2: Plot of time consumption

Time consumption can further be worked upon and can be minimized using a technique of deduplication along with the random key in the encryption process. Time consumption also greatly depends on the speed with which internet works. The slow speed of the internet causes higher time consumption than lease line internet connection.

V. CONCLUSION

Cloud computing not only provides the resources to the users but also give a big challenge to security. There are securities requirements for both users and cloud providers but sometimes it may conflict in some way. Security of the cloud depends upon trusted computing and cryptography. In our review paper some issues related to data location, security, storage, availability, and integrity. Establishing trust in the cloud security is the biggest requirement. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has a bright future.

REFERENCES

[1] F. Sabahi, "Cloud Computing Security Threats and Responses," pp. 245–249, 2011.

[2] X. Wu, R. Jiang, and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," pp. 1–14, 2015.

[3] J. Aikat *et al.*, "Rethinking Security in the Era of Cloud Computing," no. June, 2017.

[4] K. Hwang, X. Bai, Y. Shi, M. Li, W.-G. Chen, and Y. Wu, "Cloud Performance Modeling with Benchmark Evaluation of Elastic Scaling Strategies," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 130–143, Jan. 2016.

[5] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.

[6] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, p. 50, 2010.

[7] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," *Proc. - 10th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2008*, pp. 5–13, 2008.

[8] S. J. Nirmala, N. Tajunnisha, and S. M. S. Bhanu, "Service provisioning of flexible advance reservation leases in IaaS clouds," vol. 3, no. 3, pp. 154–162, 2016.

[9] M. Marwan, A. Kartit, and H. Ouahmane, "Secure Cloud-Based Medical Image Storage using Secret Share Scheme," 2016.

[10] D. V. Dimitrov, "Medical internet of things and big data in healthcare," *Healthc. Inform. Res.*, vol. 22, no. 3, pp. 156–163, 2016.

[11] J. Li, J. Li, X. Chen, C. Jia, W. Lou, and S. Member, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," pp. 1–12, 2013.

[12] S. Seo, M. Nabeel, and X. Ding, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," pp. 1–14, 2013.

[13] S. Wang, J. Zhou, J. K. Liu, J. Yu, and J. Chen, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing," vol. 6013, no. c, pp. 1–13, 2016.

[14] D. Xu, C. A. I. Fu, G. Li, and D. Zou, "Virtualization of the Encryption Card for Trust Access in Cloud Computing," vol. 5, 2017.

[15] A. Alabdulatif, H. Kumarage, I. Khalil, M. Atiquzzaman, and X. Yi, "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure," *IET Wirel. Sens. Syst.*, vol. 7, no. 6, pp. 182–190, 2017.

[16] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE : Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage," vol. 1374, no. c, pp. 1–12, 2016.

[17] L. Jiang, D. Guo, and S. Member, "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage," vol. 5, 2017.

[18] C. Liu, S. Member, L. Zhu, J. Chen, and S. Member, "Graph Encryption for Top-K Nearest Keyword Search Queries on Cloud," vol. 3782, no. c, pp. 1–11, 2017.

[19] C. Song, Y. Park, J. Gao, S. K. Nanduri, and W. Zegers, "Favored Encryption Techniques for Cloud Storage," pp. 267–274, 2015.

[20] N. Veeraragavan, "Enhanced Encryption Algorithm (EEA) for Protecting Users ' Credentials in Public Cloud."

[21] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight Searchable Public-key Encryption for Cloud-assisted Wireless Sensor Networks," *IEEE Trans. Ind. Informatics*, vol. XX, no. XX, pp. 1–12, 2017.

[22] K. L. Tsai *et al.*, "Cloud encryption using distributed environmental keys," *Proc. - 2016 10th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2016*, pp. 476–481, 2016.

[23] A. El-yahyaoui, "A verifiable fully homomorphic encryption scheme to secure big data in cloud computing," 2017.

[24] G. Thomas, "Cloud computing security using encryption technique," pp. 1–7.