Comparative Study of Fully Homomorphic Encryption and Fully Disk Encryption schemes in Cloud Computing

[1]Akriti Sharma, [2]Nagresh kumar

[1]Meerut Institute of engineering and technology, Meerut, Uttar Pradesh, India
[2]Meerut Institute of engineering and technology, Meerut, Uttar Pradesh, India

ABSTRACT— *The cloud can offer services to the users at lower cost and services are available at anytime, anywhere, user data security is the main challenge in cloud computing. The data encryption is the best way for providing data security in cloud computing. Two encryption schemes come into existence: Fully disk encryption scheme (FDE) and fully homomorphic encryption scheme (FHE). In this paper, comparison is made between the two on certain factors which conclude that fully homomorphic encryption scheme is more reliable and provides more security as compare to fully disk encryption scheme. The main problem with fully disk encryption scheme is key management, key storage, and data aggregation and so on. To solve the problem of key management and key sharing various schemes are proposed in last few years. The various securities are possible in these schemes. The third party auditor is the scheme for key management and key sharing. The third party auditor scheme will be failed if the third party's security is compromised or third party will be malicious. So, in this paper we have made comparative study between fully Homomorphic Encryption and Fully Disk Encryption schemes used in cloud computing for data security.*

KEYWORDS— *cloud computing, data storage, FDE, FHE, security, third party auditor.*

I. INTRODUCTION

Cloud computing is environment which give convenient and on demand network access to a shared pool of computing resources like servers, networks, applications, storage and services that can be quickly released in an efficient way. The word cloud stands for internet, along these lines cloud computing means internet based computing. Cloud is a centralized database where numerous clients/organizations store their data and conceivably modify data and retrieve data [7]. Cloud is a model where services are provided by CSP (cloud server provider) on pay per user base to user, means here customer needs to pay just for what he is utilizing or being served. Cloud computing is a system which give a colossal range of applications under various sort of topologies and each topology drives some new specialization. Indeed, even cloud service provider like Drop box could accidently permits accessing any user's account without user knowledge. This would potentially lead to massive data breaches which are beyond user's control [4].

To fortify the security for cloud computing most organizations embrace standard enterprise security solutions like firewall, IPS, and antivirus. Since users can now access cloud services from anyplace around the globe. A few organizations may execute strong user verification and access control solutions as a defense against personality frauds. Tragically, these solutions don't really protect the user's data in the cloud.

The cloud computing model has three service job models and three sets up models. The three service job models are:

1) *Cloud software as a service*
2) *Cloud platform as a service*
3) *Cloud infrastructure as a service*

The three set up models are:

1) Private cloud

2) Public cloud

3) Hybrid cloud

Cloud systems are not simply one more type of resource provisioning infrastructure that will enable further types of applications and truth be told, have multiple opportunities from the principles for cloud infrastructures that will enable further types of applications, reduced development and provisioning time of different services. Cloud computing has particular characteristics that recognize it from classical resource and service provisioning environments [14]:

1) *Infinitely (more or less) scalable*
2) *Cost saving/less capital expenditure*
3) *Higher resource utilization*
4) *Business agility*
5) *Disaster recovery and backup*
6) *Device and location independence*

While reducing up-front IT cost or capital expenditure is the one of the crucial reason for the adopting the cloud computing, there are additionally some different factors that encourage the different organizations for the adoption of cloud computing.

In static resource allocation configurations there inevitably exists a trade-off between capacity deployment and resource demand. Cloud computing shifts the location of resources to the cloud to reduce the costs connected with over-provisioning (i.e. having an excessive number of resources), under-utilization (i.e. not utilizing resources enough) and under-provisioning (i.e. having too little resources). It additionally reduces the time required to arrangement resources in minutes, permitting applications to rapidly scale under-utilization both up and down, as the workload changes. Accordingly, cloud computing is particularly appropriate for applications with a variable workload that experience hourly, day by day, week by week or month to month changeability in utilization of resources. One example of such applications is online shops, which need to handle their peak loads at Deepawali time. Another example is college websites, which need to handle their peak loads amid exam result time.

In traditional (i.e. non-cloud) environments, over provisioning and under-utilization can scarcely be avoided [15]. There is a perception that in many companies the average utilization of application servers ranges from 5 to 20 percent, implying that numerous resources like CPU and RAM are sit still at no peak times [16]. Then again, if the companies shrink their infrastructures to reduce over-provisioning and under-utilization, the risk of under-provisioning will increase. While the costs of over-provisioning and under-utilization can without much of a stretch be calculated, the costs of under-provisioning are more hard to calculate in light of the fact that under-provisioning can lead to a loss of users and zero revenues [16].

As we probably am aware, cloud computing has different motivating factors as indicated by the perspective of adoption however there is still long route for cloud computing to substantiate itself as indicated by the organization's trust level. There are different reasons that cautions us for the adoption of cloud computing.

1) *Security*
2) *Difficult to migrate*
3) *Internet dependency- performance and availability*
4) *Downtime and service level*

Security issue has assumed the most important part in hindering cloud computing acceptance. Different security issues, conceivable in cloud computing are: availability, integrity, confidentiality, data access, data segregation, privacy, recovery, accountability, multi-tenancy issues et cetera. Answer for different cloud security issues change through cryptography, particularly public key infrastructure (PKI), utilization of multiple cloud providers, standardization of APIs, improving virtual machines support and legal support [14], [17]. It's not simple to move the applications from an enterprise to cloud computing environment or even inside different cloud computing platforms on the grounds that different cloud providers support different application models which are likewise dissimilar from enterprise application structures [14]. A cloud computing service relies completely on the availability, speed, quality and performance of internet as it functions as transporter in the middle of consumer and service provider [14]. In business applications, downtime is regular concern in light of the fact that each minute of downtime is minute in which important business application can't be performed which degrades the performance of organization too reputation additionally [14].

II. LITERATURE REVIEW

There are several techniques for data security and privacy in the cloud computing. One of the techniques for cloud data security and methods proposed for ensuring data security is by using TPA (Third Party Auditor). Third Party Auditor [1] is a kind of inspector. There are two categories: private audit ability and public audit ability. Although, private audit ability can achieve a higher amount of efficiency whereas public audit ability allows anyone not just the user or client (data owner) to question the cloud server about the correctness of data storage while keeping no private information. The data protection-as-a-service (DPaaS) [2] cloud platform architecture dramatically reduces the per-application development effort required to offer data protection while still allowing rapid development and maintenance. The DPaaS approach moves key management and access control to a middle tier of the computing platform to balance rapid development and easy maintenance with user side verifiability.

Although cloud computing has many plus points, but there still exist many difficulties that need to be solved [3]. According to a survey about cloud computing, the profits in market size for public and hybrid cloud is $59 billion and it will go on to USD 149B by 2014 with a compound annual growth rate of 20. The revenue estimation implies that cloud computing is a promising industry. To prevent data access from unauthorized access, a distributed technique was proposed. The proposed techniques [4] perfectly stores the data and identifies at the cloud server and also execute some of the tasks such as data deleting, data inserting and data updating. For data protection, different data encryption schemes [5] like homomorphic encryption, searchable and designed encryption, individuality based encryption, sign based encryption are proposed. These are emerging techniques in cloud world security to provide day night full protection to critical data information.

To encrypt and decrypt the file at the user side different designs and architectures are proposed which provide security to data at rest and in addition while transferring. One of the engineering proposed is a Rijndael Encryption Algorithm alongside an EAP-CHAP [6]. From the customer perspective cloud computing security concerns particularly privacy protection and data security issues remains the primary inhibitor for the adoption of cloud computing services. So in this engineering just authorized user can access the data. Regardless of the possibility that some intruder (unauthorized user) gets access of the data accidentally or intentionally he won't have the capacity to decrypt it. Likewise it is proposed that encryption must be finished by the user to provide better security algorithm.

As we as a whole know data are shared with the cloud service provider (CSP) is identified as the core scientific problem that separates cloud computing from different topics in computing security. There are different approaches [7] to protect data from cloud infrastructure provider. One of the methods is, in which in-browser key translation permits a software-as-a-service application to keep running with confidentiality from the service provider. This investigates how trusted hardware can be utilized to protect cloud-based data. Cloud computing have a few advantages over traditional (non-cloud) environment and have the ability to handle most sudden, temporary peaks in application demand on cloud infrastructures. Virtualization technology provides good support to accomplish the aim of cloud computing like higher resource utilization, elasticity, reducing IT cost or capital expenditure to handle temporary loads and in addition cloud computing have different adaptable services and deployment models which is likewise one of the fundamental issues of adopting this computing worldview [18]. Virtualization concepts have open shared nature which is responsible for the violation of security polices and laws and also degrades their computing reputation and performance. So there is a need to concentrate on privacy and on solutions of different security problems to maintain the trust level of organization for deploying the cloud computing with no hesitation furthermore need of technical support for elastic scalability to serve by the vertical scaling approach which is at present restricted to just horizontal scaling. Cloud Computing consolidates various computing concepts and technologies, for example, Service Oriented Design (SOA), Web 2.0, virtualization and different technologies with dependence on the Internet, giving normal business applications online through the web browsers to satisfy the computing needs of users, while their software and data are stored on the servers [19]. In a few respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide [20].

III. SECURITY ISSUES RELATED TO THE CLOUD

Cloud security is security principles applied to safeguard data or file, functions and setup that is associated within the cloud computing technology. There are many security issues associated with cloud computing and they can be gathered into any number of dimensions. Cloud Security Alliance (CSA) [9] is gathering individuals that provide a solution, individuals that are not entered for the money (non-profits) to participate into a discussion about the current and future best practices for information assurance in the cloud. The CSA has identified thirteen domains of concerns on a cloud computing security.

A. Abuse and Nefarious Use of Cloud Computing

Iaas providers offer their customers the illusion of unlimited resources, systems, and data storage capacity often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using the services of the cloud. Some providers even give free fixed trial periods. By misusing the relative mysterious at the cast off these registration and usage models, spammers, malicious code authors, other criminals have been able to conduct their activities with relative freedom. PaaS providers have traditionally been affected by these kind of attacks; however recent evidence shows that hackers have begun to target IaaS retails as well. Further areas of concern are related to password and key cracking.

B. *Data Security and Confidentially issues*

One of the biggest concerns people have when moving to the cloud is related to the problem of keeping data secure and personal or private. In this way, some specific difficulties arise: who can create data, where data is stored, who can access and make changes in the data, what situation arises when data is deleted, how the back-up for data is done, how the data allocation occurs, etc. it is much more difficult for the cloud customer to effectively check the data handling public key infrastructure, etc are proposed to customer's practices of the cloud provider and thus be sure that the data is handled in a proper way. To counter such a risk, strategies like data encryption, particular as security measures to create a trusted and secure environment.

C. *Interoperability issues*

The cloud computing technology offers a degree of resource scalability which has never been reached before. Companies can benefit from additional computational needs, storage space, bandwidth allocation, etc. whenever, they need and without great investments to support peak load demands. If the demand falls back the additional capacity can be shut down just as quickly as it was scaled up without any hardware equipment sitting idle. This great advantage has also a major drawback. It comes alongside with the risk of managing data within a shared environment with other cloud clients. Additionally, at one time one company may have cloud providers for different services to another cloud and in such case the lack of interoperability can block or raise obstacles to such a process. Cloud service providers may find the customer look-in system attractive, but for the customers interoperability issues mean that they are vulnerable to price increase, quality of services not meeting their needs, closure of one or more cloud services, provider going out of business disputes between with the cloud provider.

D. *Malicious insider*

A malicious insider is a man motivated to make a terrible impact on the association's mission by taking action that trade off information confidentiality, integrity, and availability. At the point when sensitive data is processed outside the enterprise the organizational managers are less immediately aware of the nature and level of risk and they don't groups quick and direct capability to control and counter these risks. Experienced security specialists are exceedingly aware of the inverse relationship between loyalty and risk. Regardless of the possibility that trusted company employees can commit errors or commit fraud and outside are not automatically less ethical than them, it is prudent to invest company's long haul employees with higher trust.

The malicious activities of an insider could potentially affect: the confidentiality, integrity, and availability of a wide range of data and services with impact on the interior activities, association's notoriety and customer trust. This is especially important on account of cloud computing because of the way that cloud architectures require certain roles like cloud administrators, cloud auditors, cloud security personnel, which are to a great degree high risk.

IV. ENCRYPTION: FDE VERSUS FHE

To protect data from unauthorized access a standout amongst the most widely recognized methods utilized is the encryption. The reality is that encryption is simply one more tool to address the issues of data protection. As of late, fully disk encryption (FDE) and fully homomorphic encryption(FHE) computing on encrypted data have increased significant consideration. In any case, these strategies just partially react to the challenges in data security and maintenance.

A. *Fully Disk Encryption*

FDE encrypts entire physical disks with a symmetric key – frequently in disk firmware – to ensure simplicity and speed. While FDE is effective in protecting private data in certain scenarios, for example, stolen laptops and backup tapes, the concern is that it can't fulfill data protection goals in the cloud, where physical theft is not the primary threat. FDE alludes to encryption at the hardware level. It works via automatically converting the data on a hard drive into a form that can't be comprehended by anybody without the key to "undo" the conversion. Without the appropriate authentication key, regardless of the possibility that the hard disk is removed and puts in another machine, the data remains inaccessible. FDE can be installed on a computing device at the season of manufacturing, or it can be added a short time later, by means of a special driver.

B. *Fully Homomorphic Encryption*

FHE lies on the flip side of the spectrum. It supposedly offers the potential of general computation on cipher texts. At an essential level, any function in plain text can be transformed into an equivalent function in cipher text, the server does the genuine work, without knowing the data it is computing. This novel property gives solid privacy guarantees when computing on private data, however the question of its practicality for general cloud applications remains. A FHE [8] scheme permits user to perform non-interactive secure computation. In numerous applications, this feature can be crucial. Inside a cloud environment, ought to a cloud specialist co-op be untrustworthy, the user is faced with a choice: put private data at risk, or encrypt the data before uploading. Data encrypted through a FHE scheme enables the cloud to compute on the data while maintaining the privacy of that data. FHE implies encryption where plain text and cipher text are treated with an algebraic function. Structured encryption: A structured encryption scheme encrypts structured data in a manner that it can be queried using a query-particular token that must be created with knowledge of the secret key [10]. What's more the query procedure reveals no useful information about either the query or the data. The representation of the function f is an important issue. Since the representation can shift between schemes, we leave this issue outside of this syntactic definition.

C. Difference between FDE versus FHE

A comparison between FDE and FHE in the cloud computing situation reveals how these encryption strategies fall short of addressing the previously mentioned security and maintenance challenges simultaneously. Table no.2 speaks to comparison between FDE and FHE schemes.

1) Key management

With FDE, the keys might be located in with the cloud platform, generally on or near physical drive: the cloud application user isn't required in key management. While user data is encrypted on the physical disk, it is constantly accessible in the clear to any layer above it. Thusly, FDE doesn't avoid the online attacks from leaking the data to an unauthorized party, which is basic in the cloud setting than physical attacks [5]. With FHE, untrusted application can't without much of a stretch learn or break data. Users typically own and manage FHE encryption keys, while applications compute on encrypted forms of user data without actually "seeing" the data [11].

2) Sharing

Cooperation is frequently refered to as a killer feature for cloud applications. Fine grained access control is important to let a data owner specifically impart at least one data objects to other user. With FDE, users should fully trust the cloud provider to enforce correct access control on the grounds that the key granularity doesn't line up with access control granularity. With FHE, in light of the fact that the user or third party cloud provider employed by the user manages the encryption keys, the most ideal method for providing access control isn't clear yet. To offer fine grained encryption based access control, we may need to define key management on a for every data object granularity premise or different collections of data objects, those objects should at present be encrypted under a similar public key[10].

TABLE I

COMPARISON BETWEEN FDE AND FHE SCHEMES

parameter	FDE	FHE
Key management	Ideal for physical attacks; does not prevent leakage of data on account of online attacks	Users own the FHE keys; does not address the challenge of storing keys securely
Sharing	Key granularity does not line up with access control granularity; sharing is, therefore, not foolproof	With users holding and managing keys, access control is a challenge
Performance	when implemented on the disk firmware, FDE can avoid slowdown	Not yet efficient for deploying on the scale
Ease of development	No impact on application development	Developers cannot look at the data, making debugging, testing, and improvements difficult
Maintenance	When something went wrong in the system FDE can detect the problem up to some limit	If the system fails due to any reason, it require detecting problem or understanding what actually went wrong, which could be major challenge

Aggregation	Users fully trust cloud; this makes aggregation easier	Does not readily allow computing on data encrypted under different keys; aggregation is, therefore a challenge

3) Performance

At the point when FDE is implemented in disk firmware, its symmetric encryption can keep running at the disk's full bandwidth, successfully avoiding a slowdown. Despite the fact that researchers have made important advances in improving FHE's performance since Gentry's original proposal, it has a long way to go before becoming sufficiently efficient to deploy at scale.

4) Ease of development

Since FDE is hidden behind an abstraction of the physical disk, it typically has no impact on application development. In principle, FHE could likewise be relatively automatic: it works with an abstraction of the program as a circuit and transforms that circuit. In practice, in any case, performing this translation for discretionary programs—especially while marshaling data—could be very unpredictable. At any rate, programming tools would need to evolve dramatically. FHE doesn't permit developers to input data-driven judgments into the development cycle. In particular, application developers can't take a gander at the data, making debugging, A/B testing, and application improvements more difficult [12].

5) Maintenance

Bugs are inescapable. Be that as it may, availability is an essential cloud objective, they have to investigate quickly is a top need. Frameworks regularly fall flat for some unforeseen reason, obliging somebody to venture in and manually make a move. Determining the nature of the issue may require detecting unusual activity or understanding precisely what turned out badly, which isn't simple with FHE. In the event that the application writer can't inspect the application state meaningfully, debugging could be a real challenge [13].

6) Aggregation

Many cloud applications require data mining over various users' data for tasks (for example spam filtering, computing aggregate statistics). Data aggregation activities are relatively simple with FDE, since users fully trust the cloud provider. Current FHE procedures don't promptly permit computing on numerous users' data encrypted under different keys. Thusly, it isn't clear yet how to support such data aggregation applications with FHE; also, offline aggregation over users' data isn't possible. One solution may be to escrow keys to the cloud provider, yet that would eliminate a significant number of FHE's benefits, making its cost harder to justify.

From the above discussion, it is concluded FHE gives more security to the data in cloud computing as contrast with the FDE. Since FDE offers simple development furthermore has good performance however it needs in security issues as compared to the FHE.

V. CONCLUSION

Cloud computing is relatively a new concept which provides users with a large number of benefits. However cloud computing also has some pros mainly the security problems. Security problems can be solved by using encryption schemes.

In this paper, we discuss various security issues associated with the cloud computing. We study encryption techniques: Fully Homomorphic Encryption and Fully Disk Encryption schemes in cloud computing. We compare between Fully Homomorphic Encryption Scheme and Fully Disk Encryption Scheme for data security in cloud computing. In this paper, we conclude that FHE offers more data security to the cloud than FDE based on several factors like key sharing, key management, performance, aggregation, maintenance and ease of development. FDE offers top-notch performance and relative simplicity in development, though it fails to offer sufficient privacy. On the other end of the spectrum, FHE removes data visibility entirely from both the server and application developer thus providing more security of the data in cloud computing. Although FDE is better than FHE in terms of development and performance but it lacks in privacy issues which are very important for security of data in cloud computing. Thus, we conclude that FHE is better than FDE in terms of privacy and security of data in cloud computing.

REFERENCE

[1] Bhavna Makhija, VinitKumar Gupta "*Enhanced Data Security in Cloud Computing with Third Party Auditor",* International journal of Advanced Research in Computer Science and Software Engineering, 2013

[2] Dawn Song, Elaine Shi "*Cloud Data Protection for the Masses*" IEEE Computer Society,2012

[3] Devan Chen, Hong Zhao "*Data Security and Privacy Protection issues in Cloud Computing*" International Conference on Computer Science and Electronics Engineering, 2012

[4] Deepanchakaravarthi Purushothaman and Dr. Sunitha Abburu " *An Approach for Data Storage Security in Cloud Computing"* IJCSI International Journal of Computer Science Issues, Vol.9, Issue2, No 1.,2012

[5] Simarjeet Kaur " *Cryptography and Encryption In Cloud Computing"* VSRD-IJCSIT, Volume 2(3), 2012,242-249, 2012

[6] Sanjoli Singla, Jasmeet Singh "*Cloud Data Security using Authentication and Encryption Technique"* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013

[7] Mark D. Ryan , "*Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches*", 2013

[8] Zvika Brakerski ,Vinod Vaikuntanathan *"Effcient Fully Homomorphic Encryption "LWE, 2010*

[9] Sigrun Goluch "*The development of homomorphic cryptography"Vienna University of Technology*, 2009

[10] Defence Signals Directorat "*Cloud Computing Security Consideration*" *Cyber Security Operations Centre*, 2011

[11] Ponemom Institute "*Encryption in the Cloud* " Thales e-Security, 2009

[12] Anthony T. Velte Toby J. Velte, Ph.D. Robert Elsenpeter, 2010 "*Cloud Computing: A practical Approach*" 2011

[13] Fraunhofer Verlag "*These curity Of Cloud Storage Services*" Fraunhofer Institute for Secure information Technology, 2012

[14] Ajay Jangra, Renu Bala "*Spectrum of Cloud Computing Architecture: Adoption and Avoidance Issues*", International Journal of Computing and Business Research, Volume 2, Issue 2, May 2011.

[15] C. Braun, M. Kunze, J. Nimis, and S. Tai, "*Web-based Dynamic IT-Services",*Springer Verlag, Berlin, Heidelberg, 2010.

[16] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "*A view of cloud computing*" April 2010.

[17] Kuyoro S. O., Ibikunle F. & Awodele O, "*Cloud Computing Security Issues and Challenges*", International Journal of Computer Networks (IJCN), Volume 3, Issue 5, pp 247-255, 2011.

[18] Bhushan Lal Sahu, Rajesh Tiwari, "*A Comprehensive study on cloud computing*", Internatioinal Journal Of Advanced Research in Computer Science and Software Engineering,Volume 2,Issue 9,September 2012 .

[19] Ertaul L, Singhal S, Gokay S, "*Security challenges in Cloud Computing"*, International conference on Security andManagement SAM'10. CSREA Press, Las Vegas, US, pp 36–42,2010.

[20] Grobauer B, Walloschek T, Stocker E, " *Understanding Cloud Computing vulnerabilities*", IEEE Security Privacy, 2011.