SMTP GateWay- Using Homomorphic authenticator in Cloud Storage System

Gaddam hemalatha
M.Tech, Computer Science &Engineering
Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.
K.V.Nanda Kishore
Associate Professor, Department of CSE
Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.
Dr. I.Satyanarayana
PRINCIPAL
Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.

Abstract: In this work, we supply an introduction to privacy issues in Cloud Computing and discuss the state of art within the privacy improving technologies that can be used for Cloud Computing. We focus on a software as a Cloud scenario (webmail services) and suggest a privacy preserving architecture wherein users can hold their mail within the servers of their service providers in a cloud without compromising functionality (search ability of mails) or privateness. On demand which they may be able to access by way of web with out the necessity of pricey computers or a enormous storage procedure capability and with out paying any gear maintenance expenses and also when the mail is transferred from one domain to another, it is transmitted through SMTP gateway.

KeyWords: Privacy, Homomorphic Encryption, Security, Cloud Computing, SMTP.

I. INTRODUCTION

To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation turns into vital. Not too long ago, regenerating codes have gained popularity as a result of their decrease restore bandwidth while offering fault tolerance. We advise a third party auditing scheme for checking de-duplication and regenerating-code-founded cloud storage. To clear up the regeneration quandary of failed authenticators within the absence of data owners, we introduce a internet provider, which is privileged to regenerate the authenticators, into the common third party auditing approach model. Moreover, we design a novel third party auditing authenticator, which is generated by way of a couple of keys and will also be regenerated making use of partial keys. As a consequence, our scheme can wholly free up data owners from on-line burden. Cloud computing, to put it effortlessly, way ―internet Computing. The internet is customarily visualized as clouds; accordingly the time period ―cloud computing for computation accomplished through the web. With Cloud Computing clients can access database resources via the internet from wherever, for so long as they need, without traumatic about any security or administration of specific resources. Apart from, databases in cloud are very dynamic and scalable.― Cloud computing is a model for enabling easy, on-demand network access to a shared pool of configurable computing resources.

Cloud vendors like IBM, Google and Amazon use the virtualization on their Cloud platform and on the equal server can coexist a virtualized storage and cure house that belong to concurrent companies. The part of protection and confidentiality ought to intervene to secure the data from each and every of the firms, comfortable storage and remedy of data requires using a ultra-modern side of cryptography that has the criteria for cure comparable to, the necessary time to respond to any request sent from the client and the size of an encrypted data to be able to be stored on the Cloud server. Transfer the processing of your information to a third party; additionally it is transferring probably the most responsibility associated with their security and compliance. It isn't shocking that safety experts are fearful. Consequently, it's predominant that we thoroughly trust on our cloud provider. The advantages of cloud computing incorporate lowered costs, convenient protection and re-provisioning of resources, and thereby improved gains. Our concept is to encrypt data before sending it to the cloud provider, but to execute the calculations the info should be decrypted each time we have to work on it. Unless now it used to be unimaginable to encrypt information and to believe a third occasion to hold them nontoxic and in a position to perform distant calculations on them. With the intention to allow the Cloud provider to perform the operations on encrypted data without decrypting them requires using the cryptosystems situated on Homomorphic Encryption [8].

II. RELATED WORKS

H.C.H. Chen and P.P.C. Lee, "Enabling knowledge integrity safeguard in Regenerating-coding-based cloud storage: idea and Implementation." in that case [4] provide safeguard to the users data I the cloud storage against corruptions, internal or external attacks and finally including failure compensation to the cloud storage along with data integrity checking ,verification and to recuperate faults, turns into a relevant undertaking. Regenerating code presents failure toleration via segmenting logical sequential information across multiple number of servers also makes use of minimal restore traffic than natural remover for the period of failure reparation code. Seeing that we're going to talk about the difficulty of checking the integrity and verification of Regenerating-coding-based data towards internal and external attacks under an actual time life cloud storage surroundings .We design data integrity protection DIP scheme for regenerating code and the privacy retaining homes fault tolerance and repairing the minimum traffic.

F. Sabahi faculty of computer engineering Azad tuition Iran." Cloud Computing protection Threats and Responses": [5] many IT businesses going through the valuable problems corresponding to safety and integrity that exist with improved implementation with the cloud computing. These types of standards initiate which is remotely stored from the user's vicinity. Cloud computing expanded because of projecting safety hazards. Some quandary arises that clients' wants to appreciate as they must observes these things severely relocating business in the direction of cloud computing. There is an approach to clear up this problems is RAS problems. These are projected safety dangers Reliability, protection and availability.
Yuchong Hu scholar Member, IEEE, Lee, P.P.C. Scholar Member, IEEE; Shum, k.W, "analysis and building of sensible regenerating codes with uncoded repair for allotted storage techniques":[6] if so the allotted storage techniques applies the overabundance coding approaches to store their data. Redundancy can curb the repairing bandwidth. i.e., the huge quantity of data transferred when repairing a failed storage device. Present regenerating codes most likely require surviving storage nodes encode data for the duration of repair. This paper suggests the functional minimum storage regenerating (FMSR) codes, which allows the uncoded restore. Even as retaining the much less restore bandwidth ensures our data and in addition minimizing disk reads time. FMSR codes provides intended FMSR codes.

Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: applying network coding for the storage restore in a cloud-of-clouds": in that case ,this paper[7] provides fault tolerance to spread data across more than one cloud companies. However, if a cloud suffers from a permanent failure and loses all its data, it is quintessential to repair the lost data with the support of the other surviving clouds to keep data redundancy. This paper provided a proxy-based storage system for fault-tolerant more than one-cloud storage known as NCCloud, which achieves price-amazing repair for a permanent single-cloud failure. NCCloud is constructed on higher layer of community-coding-established storage and its often called practical minimum storage regenerating codes which continues fault tolerance. FMSR provides economic price saving in restore over RAID-6 codes, even as having comparable response time efficiency in cloud storage operations equivalent to add or download.

Storing the data in the cloud, can increase the privacy risks for the following stake holders:
1) Cloud Computing User
2) Organization using the Cloud Service
3) Implementers of Cloud Platforms
4) Providers of application on top of cloud platforms
5) For the data subject
This work focuses on the following threats: (a) Sharing with an unauthorized party, (b) Malicious internal users, and (c) Account or service hijacking. Our work applies to the class of cloud services that stores data and provide searching as its primary functionality. This includes services such as webmail, collaborative document authoring (Google documents) and private blogs. The example used throughout this paper is Email.

III. SYSTEM ARCHITECTURE

In this section, we review the basic elements common towebmail infrastructures.

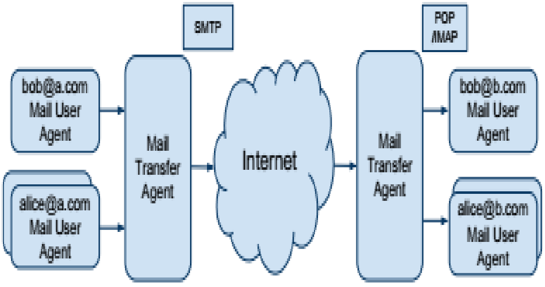

SMTP
POP /IMAP
bob@a.com Mail User Agent
alice@a.com Mail User Agent
Mail Transfer Agent
Internet
Mail Transfer Agent
bob@b.com Mail User Agent
alice@b.com Mail User Agent

Fig.1. Email Architecture

A. Mail Architecture

The webmail infrastructure is responsible for end to end delivery of email. Figure 3 presents architectural components and protocols typically used to support webmail applications

The webmail infrastructure is accountable for end to end supply of electronic mail. Fig.1 grants architectural add-ons and protocols more commonly used to support webmail purposes.

1) Accessories: This subsection describes the architectural add-ons.

Mail user Agent: The Mail user Agent (MUA) is used to manage a user’s e mail. It acts on behalf of the user to send and receive mail from the Mail transfer Agent (MTA). Widespread MUAs comprise Microsoft Outlook, Mozilla Thunderbird, Apple Mail. In a webmail approach, the MUA runs in the server and the pages are rendered as HTML pages for the browser.

Mail transfer Agent: The Mail transfer Agent (MTA) transfers messages from one server to one other. It receives e-mail both from another MTA or MUA. The transmission of electronic mail follows standardized protocols for message transfers.

2) Protocols: This subsection describes in most cases used protocols.

Simple Mail transfer Protocol (SMTP): SMTP refers to the normal for the switch of messages from one server to an additional. It is used by MUA to relay mail by way of MTA and it's also utilized by MTA to send and acquire mail between other MTAs. SMTP as a standard does not encrypt messages (except Transport Layer safety encryption is used).

Publish place of job Protocol (POP) / web Mail access Protocol (IMAP): POP/IMAP are e mail retrieval protocols that explain standards for downloading messages from the MTA for MUA. Examples of use is found with aid for POP variant three and IMAP as provided by Gmail.

3) Privacy Threats: In webmail systems, there's a server for webmail offered into the typical mail procedure (fig.1). It acts because the Mail person Agent for a number of users and manages e-mail for the entire clients. The MUA, unlike the general model (fig.1), is centralized at the server. The webmail server makes use of POP/IMAP to down load messages from MTA.

Homomorphic Encryption Applied to Cloud Computing Security: When the data transferred to the Cloud we use standard encryption ways to at ease the operations and the storage of the data. Our general suggestion used to be to encrypt the data earlier than send it to the Cloud provider. However the final one wishes to decrypt data at each operation. The user will ought to provide the confidential key to the server (Cloud provider) to decrypt data before execute the calculations required, which might have an impact on the confidentiality and privateness of data stored within the Cloud. In this paper we're proposing an software of a process to execute operations on encrypted data with out decrypting them, on the way to provide the same results after calculations as if we have labored instantly on the raw data.

Homomorphic Encryption systems are used to perform operations on encrypted data with out figuring out the confidential key (without decryption), the client is the one holder of the key key. Once we decrypt the outcome of any operation, it is the same as if we had applied the calculation on the raw data.

Definition [9]: An encryption is homomorphic, if: from Enc(a) and Enc(b) it's possible to compute Enc(f (a, b)), the place f can also be: +, ×, ⊕ and without using the exclusive key. Among the Homomorphic encryption we distinguish, consistent with the operations that permits to examine on raw data, the additive Homomorphic encryption (most effective additions of the raw data) is the Pailler [10] and Goldwasser-Micalli [11] cryptosystems, and the multiplicative Homomorphic encryption (best products on raw data) is the RSA [12] and El Gamal [13] cryptosystems.

- Ek is an encryption algorithm with key k.
- Dk is a decryption algorithm.

Dk (Ek (n) × Ek (m)) = n×m OR Enc $(x \otimes y) = \mathrm{Enc}(x) \otimes \mathrm{Enc}(y)$

DL (EL (n) × EL (m)) = n+m OR Enc $(x \oplus y) = \mathrm{Enc}(x) \otimes \mathrm{Enc}(y)$

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.

Multiplicative Homomorphic Encryption (RSA cryptosystem): The Homomorphism: Suppose x1 and x2 are plaintexts. Then,

$e_k(x_1)\, e_k(x_2) = x_1^{\,b}\, x_2^{\,b} \bmod n = (x_1\, x_2)^b \bmod n = e_k (x_1\, x_2)$

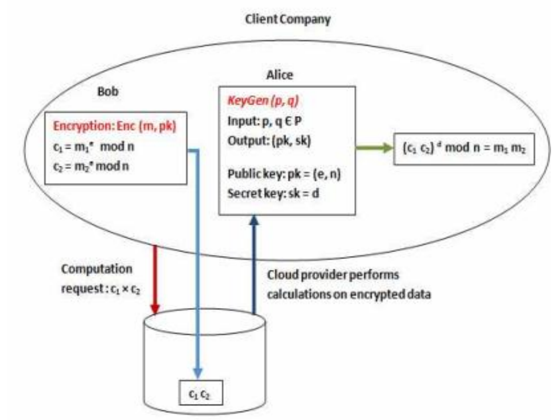


Fig.2. Multiplicative Homomorphic Encryption Applied to Cloud Computing

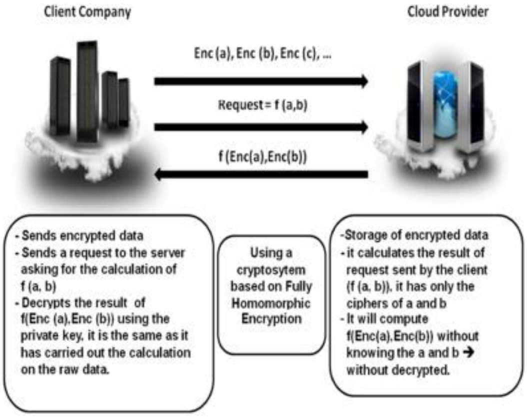
The Homomorphism: Suppose x_1 and x_2 are plaintexts. Then,

$e_k(x_1, r_1)\, e_k(x_2, r_2) = g^{x1}\, r_1^{\,n}.\, g^{x2}\, r_2^{\,n} \bmod n^2$
$= g^{x1+\,x2}\, (r_1\, r_2)^{\,n} \bmod n^2$
$= e_k(x1+ x2, r1r2)$

To perform addition and multiplication on encrypted data stored in the cloud provider, the client must have two different key generators (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.

For all types of calculation on the data stored in the cloud, we must opt for the fully Homomorphic encryption which is able to execute all types of operations on encrypted data without decryption.

Fully Homomorphic Encryption: The application of fully Homomorphic encryption is an important stone in Cloud Computing security, more generally, we could outsource the calculations on confidential data to the Cloud server, keeping the secret key that can decrypt the result of calculation.



- Sends encrypted data
- Sends a request to the server asking for the calculation of f (a, b)
- Decrypts the result of f(Enc (a).Enc (b)) using the private key, it is the same as it has carried out the calculation on the raw data.

Using a cryptosytem based on Fully Homomorphic Encryption

-Storage of encrypted data
- it calculates the result of request sent by the client (f (a, b)). it has only the ciphers of a and b
- It will compute f(Enc(a).Enc(b)) without knowing the a and b → without decrypted.

Fig.3. Fully Homomorphic Encryption applied to the Cloud Computing

IV. CONCLUSION

We proposed a privacy maintaining architecture for our webmail process, that permits secure conversation of messages utilising the security of Cloud Computing based on totally Homomorphic Encryption is a new idea of security which is enable to furnish the outcome of calculations on encrypted data with out understanding the raw entries on which the calculation used to be applied respecting the confidentiality of data. Nonetheless, our contribution is the concept of the framework. The encryption algorithms used will also be modified to make use of extra comfortable choices in our architecture.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian, "Privacy-Preserving Public Auditing forRegenerating-Code-Based Cloud Storage," IEEE TRANSACTIONS ON INFORMATION AND SECURITY, vol. 1, Nov. 2015.

[2] Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," IEEE TRANSACTIONS ON CLOUD COMPUTING, vol. 2, pp. 43-56, January-March. 2014.

[3] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE TRANSACTIONS ON COMPUTERS, vol.62, pp. 362-375, Ferbruary. 2013.

[4] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, " Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", in IEEE INFOCOM, 2010, pp. 1-15. 2009.

[5] F. sabahi Faculty of computer engineering Azad University Iran." Cloud Computing Security Threats and Responses".

[6] Yuchong Hu Student Member, IEEE, Lee, P.P.C. Student Member, IEEE; Shum, K.W, "Analysis and construction of functional regenerating codes with uncoded repair for distributed storage systems".

[7] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloud-of-clouds".

[8] Sigrun Goluch, "The development of homomorphic cryptography From RSA to Gentry's privacy homomorphism", http:// dmg.tuwien.ac.at/ drmota/DA_Sigrun%20Goluch_FINAL.pdf, 2011.

[9] Ronald L. Rivest, Leonard Adleman, and Michael L. Dertouzos. "On Data Banks and Privacy Homomorphisms", chapter On Data Banks and Privacy Homomorphisms, pages 169-180. Academic Press, 1978.

[10] Pascal Paillier, "Public-key cryptosystems based on composite degree residuosity classes", In 18th Annual Eurocrypt Conference (EUROCRYPT'99), Prague, Czech Republic, volume 1592, 1999.

[11] Kun Peng, Colin Boyd, Ed Dawson, "A Multiplicative Homomorphic Sealed-Bid Auction Based on Goldwasser-Micali Encryption", Volume 3650, pp 374-388, Springer, 2005.

[12] R. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public key cryptosystems". Communications of the ACM, 21(2): 120-126, 1978. Computer Science, pages 223-238. Springer, 1999.

[13] Osman Ugus and al. "Performance of Additive Homomorphic EC-ElGamal Encryption for TinyPEDS", 6th Fachgespräch Drahtlose Sensornetze, pp. 55--58, July 2007.

Author's Profile

Gaddam hemalatha pursing M.Tech in Computer Science & Engineering from **Sri Indu Institute of Engg. & Tech,Sheriguda(Vi),IBP(M),RR Dist.**

K.V.Nanda Kishore working as Associate professor, Department of CSE in **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi),IBP(M),RR Dist.**

Dr. I.Satyanarayana Completed B.E-Mechanical Engg. from Andhra University, M.Tech Cryogenic Engg. Specilization-IIT Kharagpur, Ph.D-Mechanical Engg.-JNTUH, Currently working as a Principal at **Sri Indu Institute of Engg. & Tech, Sheriguda(Vi), IBP(M),RR Dist.**