A Survey On Security Using Encryption Techniques In Cloud

Gaurav Jain, Vikas sejwar
P. G. Scholar
Department of CSE & IT
Madhav Institute of Technology and Science Gwalior

***Abstract*— Cloud computing (CC) is an emerging area of computer technology that benefits from the processing power and the computing resources of many connected, geographically distanced computers connected via Internet. Cloud computing promotes availability, zero maintenance, and subscription based service. In this paper define about cloud deployment models, service delivery models of cloud computing, characteristic of cloud, cloud computing adopting risks, technology, cloud computing security problem and data encryption using RSA, DES and AES.**

Keywords—cloud computing; model; security; data encryption; RSA.

I. INTRODUCTION

Cloud computing is enabling convenient model. More and more organizations and users are attracted by its low-cost and high-quality services to out-source their data to the cloud server. However, as the cloud users and servers of cloud are in different trusted domain, the cloud servers are able to control and monitor the outsourced data as well as the communication between users and servers. A lot of techniques have been investigated to protect data privacy, storage and communication security. To protect data privacy and prevent unsolicited access, a natural approach is to encrypt the sensitive data which brings great challenges to effective data utilization. In similar way, cloud server should provide the similar function to the data users, while the data and search privacy should be protected. How to apply the traditional plaintext search in the encoded information remains a most difficult task because of inherent security obstacles, including various strict requirements such as data privacy, index privacy, keyword privacy. With the arrival of 4G technologies and the development of 5G technologies, the mobile and wireless devices have profoundly changed people's life. More and more mobile applications produce massive sensitive data such as health and location information in cloud computing. It is additional complex to search over encoded information for mobile devices without strong computational capability. Therefore, secure index and search method have great potential which can simultaneously provide an ability of searching on encoded message and protect the data privacy in Cloud computing with mass mobile devices [1].

Fig.1 cloud computing

II. CLOUD DEPLOYMENT MODELS

There are various clouds types which can be subscribe to the depending on user requirement.

A. Public Cloud – Public cloud can recover by any subscriber with the internet connection and access of cloud space.

B. Private Cloud- A private cloud is recognized for a specific organization or group and limits access to just that a group.

C. Community Cloud - A community cloud is shared among various organizations which have same cloud need.

D. Hybrid Cloud - A hybrid cloud is a various cloud's combinations, where clouds are a mixture of all public, private, or community cloud.

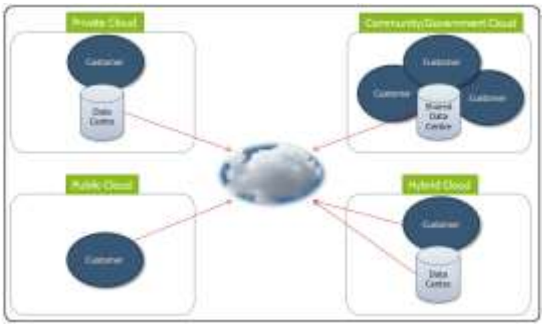

Fig.2 Models of cloud computing

III. CLOUD COMPUTING SERVICE DELIVERY MODELS

Cloud computing gives three different fundamental service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS):

A. *Infrastructure as a service (IaaS):* Cloud computing recommend virtual and physical computers, additional storage networking strategy etc. The virtual machines are run through hypervisors which is organized into controlled and pools through operational support technique.

B. *Platform as a service (PaaS):* refers to computing platforms like as web servers, databases operating systems and programming atmosphare, where cloud user uses a software or platforms offers through CSP.

C. *Software as a Service (SaaS):* Cloud users can use software that is already running and installed on cloud infrastructure. The basic cloud computing concern users is the data stored or transmitted protection to the cloud [3].

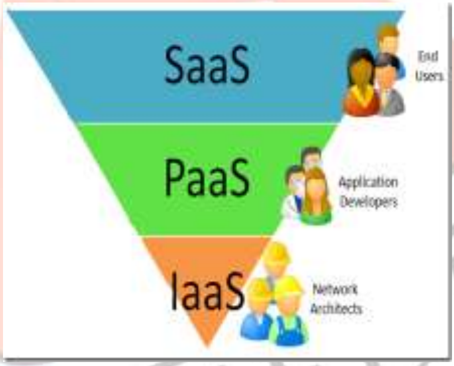

Fig. 3 cloud computing fundamental model

IV. CHARACTERISTIC OF CLOUD

The important five characteristics of Cloud computing include [3]:

A. *Service on demand:* This property involves valid customers applying a web site or interface of similar control panel for example additional computers, network bandwidth or user email accounts, no requiring any kind of interaction between customers and the Cloud Service Provider.

B. *Internetworking:* Internetworking enables a user to the access computing resources over networks like as internet from a broad computing devices range like as laptops and smart phones.

C. *Virtualization of resources:* This characteristic of virtualization conclude vendors applying shared computing resources to provide cloud services to multiple customers. Virtualization and multi-tenancy method are classically used to the both protect and segregate all customer and their information from various customers, and to create it appear to customer that they are the only user of a shared computer or software application.

D. *Flexible processing:* This property enables the rapid and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth as required by customer demand.

E. Pay-for-use service: This pay – for - use service make customers only pay for the computing resources that they actually use, and being able to monitor their usage. security of cloud computing[4].

Cloud computing offers potential benefits like cost savings and improved business outcomes for the business concerns. To maintain secure service for client, organizations should review presented security practices and employ more ones to guarantee for data security.

Corporate companies and individuals are concerned about how security and compliance integrity can be maintained in this new environment .In a Cloud computing several methodology concluding networks, databases, OS, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. The important keys to security of Cloud computing Security, Confidentiality, Authenticity, Privacy and Integrity of stored information in cloud.

Security refers to Confidentiality, Integrity and Availability, which pose big issues for Cloud Service Providers. Underpinning confidentiality goal are authentication approach like user-IDS and passwords which uniquely identify an information system's users, and supporting control approach that limit all identified user's access to data Integrity of cloud data includes only preservation without corruption of whatever was transmitted or entered into the system. Availability refers to the availability of cloud data [4].

V. RISKS OF ADOPTING CLOUD COMPUTING TECHNOLOGY

The secure cloud space creating and managing is a most difficult task as compare to the creating a secure classical IT environment. Provide the immaturity of these technology new resources and classical reallocation ones are not completely tested and come with novel risks that are still under research. The Cloud computing adopting risks identified by this paper are:

A. *Misunderstanding responsibilities*

If in a traditional scenario the security of data is completely the burden of the company owning data. In the scenario of Cloud computing responsibilities are separated between two different actors: the cloud provider and the client.

B. *Data security and confidentiality issues*

One of the biggest security concerns people have when moving to the cloud is related to the problem of keeping data secure and confidential. In this respect, few specific issue arise: who can make information, where information is stored, who can access and change data, what happens when data is deleted, how the back-up is done, how the data transfer occurs, etc

C. *Lack of Standards*

The immaturities of this technology create it difficult to develop a comprehensive and commonly accepted set of standards. As a result, many improvements were established in order to research and develop the specifications.

D. *Interoperability issues*

Cloud computing technique provides a resource scalability degree 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.

E. *Reliability breakdowns*

Cloud computing is the services reliability or availability. The breakdown of an essential service operating in a cloud has an impact on many clients. The company first said that it affected less than 2 % of their customers, then they updated to 10 %, which sums around 35 million clients of a total of 350 million users. These incidents are not rare and evidence the customer lack of control over their data

F. *Malicious insider*

A malicious insider is a someone motivated to generate a bad impact on organization’s mission through taking action which compromises data confidentiality, integrity, and/or availability. When sensitive data is processed outside the enterprise the organizational managers are less immediately aware of the nature and level of risk and they do not possess quick and direct capability to control and counter these risks [5].

VI. SECURITY ISSUES IN CLOUD

In present days, cyber warfare is debatably most difficult challenge in a multi- tenant and distributed atmosphere. It is a difficult job within client-server architecture. When information transfered to the cloud services, necessities of security should be most important. The ENISA itemize risks, recommendations and cloud computing profit. It also lists the disease on confidential document, governance loss, malicious insider, and unconfident unfinished data. It examines which data type classically found in sharing apps, riskiest exposure, and what phase take to the mitigate these security issue. The CSA and ElasticaQ2 2015 also examine how to build an effectual cloud app security architecture, which gives control, remediation and visibility.

- Software security: It provides software security idea come from engineering software dept. that it continues to function properly under malicious activities. To build a cloud atmosphere a central and critical issue is software security issue. It defects with security concluding implementation bugs, buffer overflow, designed flaws, error handling promises and much more.
- Infrastructure security: The fundamental and common challenges are to show that virtual and physic infrastructure of cloud can be trusted. The attestation of the third party is not enough for critical business procedure.
- Storage security: In the cloud storage technique, data stores on end user in cloud and also no longer owns information and where it's stored. This all the time has been an important part of QoS.
- Network security: In cloud computing, communication is via the internet and it is the cloud atmosphere backbone. Network security concerns about both external and internal attacks. These attacks in the network can either happen in the virtual or physical network. Hanqian W., et al. focused on the, in effect, virtual network in the Xen platform through discuss security issue [6].

VII. DATA ENCRYPTION USING RSA, DES AND AES

RSA

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman define a cryptographic algorithm, which was basically to swap less secure NBS algorithm. RSA is motivated through published works of Diffie and Hellman from few years before, who explain the idea of such an algorithm, but never truly developed it.

Define at the time in which era of e-mail was probable to soon arise, RSA implemented two different important ideas:

A. Public-key encryption.

This idea defined the requirements of a “courier” to deliver keys to the recipients over another protect channel before originally-intended information transmitting. In the RSA, encoded keys are public, while the decoded keys are not, so only person with the correct decryption key can decipher an encrypted data. Everyone has their own encode and decode keys. The keys must be create in such a way that decode key may not be simply deduced from the public encode key.

B. Digital signatures

The receiver may require verifying that transmitted information actually originated from sender (signature), and didn’t just come from there (authentication). This is complete applying sender’s decode key, and signature can later be verified through anyone, applying corresponding public encryption key. Signatures therefore cannot be forged. Also, no signer can later deny containing signed the information [7].

Information stored in the cloud is encrypted applying an asymmetric algorithm before storage to enforce information integrity in cloud atmosphere. The algorithm follows public key cryptography which has public and private key one for encode side and another is decode side.

C. Key generation: Every user generates a uniquepublic/private key pair by:

- Selecting two large primes at random - p, q
- Computing their system modulus
  $N= p.q$
  Note: $ø (N) = (p-1) (q-1)$
- Choose at random encode key e where
  $1<e<ø (N)$, gcd (e, $ø (N)$) =1
- Resolve following equation to the discover decode key d
  $e.d$=1 mod $ø (N)$ and $0≤d≤N$
- Publish their public encode key:
  $KU= \{e, N\}$
- Keep secret decode key:
  $KR= \{d, p, q\}$

D. Usage of Keys: To encrypt a message M, the Sender:

- Obtains public key of recipient $KU=\{e,N\}$
- Computes: $C=Me$ mod N, where $0≤M<N$

To decrypt the cipher text C, the Receiver:

- Uses their private key $KR=\{d,p,q\}$
- Computes: $M=Cd$ mod N

This enforces client information privacy over cloud and generates other users not to access the original cloud data since it has been encoded [4].

Data Encryption Standard (DES)

DES is a block cipher that uses shared secret key for encode and decode purpose. DES encryption approach is defined through Davis R. obtain a fixed-length string which is transforms it by a complicated operations series into the bit of cipher text string. In DES case, all block size is 64 bits. DES uses 56 bits key for encryption, so that decode procedure can only be execute through those who know key which is used for encrypt the information. Broad level phase in the DES are as follows:

1) In first phase, 64-bit plain text data is handed over to an IP function.
2) The IP is achieving on plain text.
3) The IP produces two different halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4) RPT and LPT go through encoding process 16 rounds.
5) RPT and LPT are rejoined and a final Permutation (FP) is achieving on combined block.
6) The outcomes of this procedure produce 64-bit cipher text. Rounds: All of the 16 stages, in turn, consist of the broad level steps.

Advanced Encryption Standard (AES)

The AES algorithm is a symmetric-key algorithm; means same key is used for both encode and decode the message. Feistel networks do not encode complete block per iteration, e.g., in DES, 64/2 = 32 bits are encode in one round. AES, on other hand, encode all 128 bits. This is one explanation why it has a comparably less number of rounds

Encoding Round Decoding Round All processing Round involves four steps:-

Substitute byte: A non-linear substitution step wherever all byte is replaced with another byte applying lookup table.

Shift rows: A transposition phase in this step all row of state is shifted regularly various numbers of steps.

Mix column: this operation is the state columns, combining four bytes in the all column.

Add round key: all state byte is XOR with round key applying bitwise.

Decryption: Decryption concludes reversing of every step taken in encode applying inverse functions like InvSubBytes, InvShiftRows, InvMixColumns [16].

VIII. LITERATURE SURVEY

Yong Yu (2016) et. al presented concrete construction from RSA signature can support variable-sized file blocks and public auditing. Here provide a formal security model for IDCDIC and prove security of our construction under RSA assumption with huge public exponents in random oracle model. We demonstrate the presentation of our proposal through developing a prototype of the protocol. Implementation outcomes present that proposed ID-CDIC protocol is practical and adoptable in real life [8].

M. Vijayalakshmi (2016) et. al presented a mechanism known as “automatic healing of services in a Cloud computing atmosphere” in which server downs are avoided and in turn, preserving message loss. To prevent message loss at the time of server crashes, we implemented a technique of two different folds. One is monitoring procedure running on Port/PID, checking CPU, Disk and memory within instance and receiving respective actions. Another one is automating procedure mentioned in the first step. While monitoring, we got to know which service reaches CPU utilization 90%. Then automatic resume of such service takes place, avoiding server downs. One more contribution of our paper is users can describe their own rules based on which actions will be triggered according need. We implemented our technique in AWS cloud where Cloud Watch is the monitoring tool. Likewise the proposed technique can be implemented in any of the clouds. Compared with the previous efforts, our process is effective and yields improved outcomes [9].

Mohammed Amoon (2016) et. al presented an adaptive framework to the cope problem of fault tolerance in Cloud computing atmosphere. The framework employs both replication and check pointing approaches in order to gain a reliable platform for carrying out customer requests. Also, algorithm determines the most appropriate fault tolerance technique for every selected virtual machine. Simulation experiment is carried out to evaluate framework’s performance. The outcomes of the experiments present that proposed framework enhance cloud performance in conditions of throughput, overheads, monetary cost, and availability [10].

Abderrahim El Mhouti (2016) et. al presented that in this paper, through taking advantage of Cloud computing services, we propose to design a flexible cloud-based VCLE. The basic goal of this proposed work exploit Cloud computing potentials to facilitate collaborative information construction and maximize resource sharing in VLE. The proposed platform fulfills basic VLE requirement to support collaborative learning, but also responds to learner’s dynamic need on demand. The platform facilitates and supports students to fulfill task-driven learning in an additional flexibly and friendly collaborative manner [11].

Peidong Sha (2016) et. al presented that, we design a encoding approach, this encoding approach firstly discriminates whether private and public key values generated at the time of the encoding procedure contain prime number, then combines with the Pascal’s triangle theorem and RSA algorithm model and inductive technique to construct a new cryptosystem that meets homomorphic computation of some operations on cihpertexts (e.g., additions, multiplications), Thus the novel cryptosystem satisfies completely homomorphic encryption in (CC)[12].

Mr.V.Biksham (2016) presented a high security encrypted data is proposed applying “somewhat” and “fully homomorphic” encryption technique. CSP provide security and privacy to the cloud users by cryptographic encryption algorithms. Through applying query any user can information access from cloud servers through decryption. But frequent decryption of cipher text may lead to exploit the integrity and authentication. To provide security to encoding data with computations, a secure encryption approach known as homomorphic encryptions which provides calculations on encoding information without decrypt cipher text and improve cloud services performance[13].

Nitin Naik (2015) et. al presented a working prototype and critical analysis of these three open standard identity protocols SAML, OIDC and OAuth. It also explores evaluation criteria which are used for this analysis purpose. In conclusion, it discusses their limitations and strengths, and establish most appropriate open standard identity protocol for all types (CC)models [14].

Viney Pal Bansal (2015) et. al presented hybrid Cryptosystem applying Blowfish and RSA algorithm. This approach provides features of both symmetric and asymmetric cryptography [15].

IX. CONCLUSION

Cloud computing is an emerging technology. It is an attractive solution when the infrastructure or the IT personnel are not available or too expensive; but it has its drawback. The disadvantage can be mostly found in the secure threats and cloud computing vulnerabilities. Unlike classical solutions where threats come from two known sources inside or outside the network; Cloud computing security threats might originate from different sources. In this paper define about cloud deployment models, cloud computing service delivery models, characteristic of cloud, risks of adopting cloud computing, technology, security issues in cloud and data encryption using RSA, DES and AES.

References

[1] Hanbing yao, Nana xing, Junwei zhou,Zhe xia, “secure index for resource-constraint mobile devices in cloud computing”, 2169-3536 2016 ieee./ volume 4, 2016.

[2] Alexa Huth and James Cebula, “The Basics of Cloud Computing”, © 2011 Carnegie Mellon University. Produced for US-CERT

[3] M. Turab1 , Anas Abu Taleb 2 Shadi R. Masadeh, “(CC)Challenges And Solutions”, Doi : 10.5121/Ijcnc.2013.5515.

[4] M. Gobi and R. Sridevi, “An Approach for Secure Data Storage in Cloud Environment”, *International Journal of Computer and Communication Engineering, Vol. 2, No. 2, March 2013*

[5] Florin OGIGAU-NEAMTIU, “(CC)SECURITY ISSUES”,

[6] Saurabh Singh, Young-Sik Jeong and Jong Hyuk Park,” A Survey on Cloud Computing Security: Issues, Threats, and Solutions”, Journal of Network and Computer Applications 2016

[7] Evgeny Milanov, “The RSA Algorithm”, 3 June 2009

[8] Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang, Zhang, Athanasios V. Vasilakos, Jian Shen, “Cloud data integrity checking with an identity-based auditing mechanism from RSA”, S0167-739X(16)30016-4/January 15, 2016

[9] M. Vijayalakshmi, D. Yakobu, D. Veeraiah, N. Gnaneswara Rao, “Automatic Healing of Services in (CC)Environment”, ISBN No.978-1-4673-9545-8/2016

[10] MOHAMMED AMOON, “Adaptive Framework for Reliable (CC)Environment”, 2169-3536 2016 IEEE

[11] Abderrahim El Mhouti, Azeddine Nasseh, Jose Marfa Vasquèz, “Cloud-based VCLE: a Virtual Collaborative Learning Environment Based on a (CC)Architecture”, 978-1-5090-4926-4/16©2016 IEEE.

[12] Peidong Sha , Zhixiang Zhu, “THE MODIFICATION OF RSA ALGORITHM TO ADAPT FULLY HOMOMORPHIC ENCRYPTION ALGORITHM IN CLOUD COMPUTING”, 978-1-5090-1256-5/16/2016 IEEE.

[13] Mr.V.Biksham, Dr. D.Vasumathi, “Query based computations on encrypted data through homomorphic encryption in (CC)security”, 978-1-4673-9939-5/16©2016 IEEE

[14] Nitin Naik , Paul Jenkins, “An Analysis of Open Standard Identity Protocols in (CC)Security Paradigm” 978-1-5090-4065-0/16/2016

[15] Viney Pal Bansal, Sandeep Singh, “A Hybrid Data Encryption Technique using RSA and Blowfish for (CC)on FPGAs”, 978-1-4673-8253-3/15/©2015 IEEE.

[16] Yogita Verma and Neerja Dharmale,” A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard”, International Journal of Science and Research (IJSR) 2013