International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-6, Issue-3, May 2018
DOI: 10.21276/ijircst.2018.6.3.3

A Survey on Various Security Issues and Challenges to Secure Cloud Computing

Rohini H. Joshi, Divya P. Rathi, Asma Khan, Medha Jain

Abstract— **Cloud computing has evolved as one of the most powerful approach in the IT industry. It provides so many advantages like minimum expense, great performance, availability of resources, due to which it is considered as revolution amongst organizations. In cloud computing various resources are shared through network in open environment so that the user can access the information from anywhere, but there exist the issues of security and privacy of user and its information. It also provides a broad study on the issues and challenges of security .Growth of cloud computing is mainly decreased due to these concerns and challenges. Even though there is secure Homomorphic encryption there lays certain security issues and attacks with it. This paper deals with the analysis of security issues on cloud computing and finding counter measures on those issues. The fundamental security issues such as confidentiality, integrity, availability, trust and audit and compliance is analyzed and the impact on each characteristics of cloud computing as well as the third party control has been examined.**

Index Terms— **Cloud Computing, Security Issues, Homomorphic encryption, Counter measure.**

I. INTRODUCTION

Cloud is defined as the computing based network on internet. Cloud Computing is an emerging technology in today's world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing provides the resources as well as services as per the need of organization or people. It is mostly used for the storage services to reduce the overhead of the hardware storage and make resources remotely available on the internet. Data or information has always been a major property for any Organization or industry. People always try to save or hide their information on secure places so that no one can access them except them. The "Five essential Characteristics" of cloud computing are:

1. Pooling of resources
2. Expansion or rapid elasticity
3. Broad network access
4. On-demand self service
5. Measured service

A public cloud is basically the internet, used by general people. It is owned and managed by cloud provider. Public cloud facilitates access to IT resources on a "pay as you go" billing model. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google App Engine and Windows Azure Services Platform [2]. Cloud computing is divided into different types:

1. Private Cloud: Private cloud refers to a model of cloud computing where IT services are provisioned over Private IT infrastructure for the dedicated use of a single organization. It provides flexibility, scalability, provisioning, automation and monitoring to maintain own data centre. Examples are Eucalyptus, Ubuntu Enterprise Cloud, Amazon VPC, etc [2].
2. Hybrid Cloud: Hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as needed [2].
3. Community Cloud - A community cloud is a cloud service model that provides a cloud computing solution to a limited number of individuals or organizations that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider [2].

According to survey, most of people use private cloud services as it provides security, stability and redundancy. Due to its cost private cloud is not suitable for large organization, they can also thing of public cloud as it also provides all the services but major concern security of information of an organization.

Manuscript Received April 28, 2018.

Rohini Joshi, Assistant Professor, Department of Information Technology,Shri Ramdeobaba College of Engineering and Management, Nagpur ,India. Mobile No.:-+91-9766948002, e-mail: joshirh@rknec.edu

Divya P. Rathi,UG Scholar, Department of Information Technology , Shri Ramdeobaba college of engineering and management, Nagpur, India, 9405526010,

Medha Jain, UG Scholar, Department of Information Technology , Shri Ramdeobaba college of engineering and management, Nagpur, India, 8237715929

Asma Khan, UG Scholar, Department of Information Technology , Shri Ramdeobaba college of engineering and management, Nagpur, India, 8793667740

II. LITERATURE REVIEW

Rachna Jain, Sushila Madan,Bindu Garg [1] in 2016, "Homomorphic Framework to Ensure Data Security in Cloud Environment", tells about the cryptographic techniques that can be used as secure storage which can help cloud computing at some extent also focuses on the major disadvantage of secure storage that it cannot perform processing on encrypted data, this problem is sort out using homomorphic encryption as in homomorphic encryption data is stored as cipher text and processing is performed on this cipher text. So there is no risk of data exposure. The proposed framework deals with the searching efficient data so as to protect it from beginning to end i.e. from uploading that data to cloud to obtaining the same data by the user. Separate approach of Performance analysis has been carried out.

Khalid el makkaoul ,Abdellah ezzati, Abderrahim beni hssane [2] "Challenges of Using Homomorphic Encryption to Secure Cloud Computing" IEEE@2015 presents the operations and categories of Homomorphic Encryption and also briefly explains about the challenges faced during adoption of algorithm. To prevent the data exposure, a homomorphic encryption performs the operations on encrypted data without disclosing the secret key during adoption of algorithm numerous challenges that may be encountered are efficiency of system, robustness, delay of processing server etc. In order to provide the solutions to these challenges improved performance of Homomorphic Encryption Systems is expected, that can be done using intelligent multi-agent systems at Cloud processing servers. The MAS (multi-agent systems) not only improve the performance and quality of service but also helps in making decisions when interacting with the external environment.

Prachi Garg ,Dr.Sandeep Goel,Dr.Avinash Sharma [3], "Security Techniques for Cloud Computing Environment", describes the problem of data security has been investigated it also highlights the existing security attacks on the basis of Amazon EC2 cloud. The attacks on web applications such as SQL injection attacks, Man-in-middle attack, Cross site scripting attacks, the security attacks at network level such as DNS attack, Sniffer attack and at application level such as Denial of service attacks, Cookie poising, Backdoor attacks etc has been discussed. It proposes a system using two different protocols i.e. DES and AES and compared the result to solve the above mentioned security issues.

Akshay Nayak, Sridhar.N.K, poornima.G.R, Dr. Shivashankar [4], "Security Issues in Cloud Computing and its Counter measure" May 19-20, 2017 describes various security issues and the counter measures to resolve those issues. It also discuss about the characteristics of cloud computing how it is used in today's world. It tells about threats on confidentiality of data or information. This paper proposed the "Threat Protection System Using Self-Destructive Mechanism" for data security on cloud. The paper had also explained the theoretical approaches of all the threats related to cloud and their solutions. They had done the comparison between different security measures and their solution which will be effectively used.

Naim Ahmad [5], "Cloud Computing: Technology, Security Issues and Solutions", discussed about the Cloud Security Issues, Multi-level Integrated Security, Service Level Agreements (SLA) and Cloud Computing Technology Framework. The paper proposed different researches on cloud, its threats, its technology, challenges and barriers to adopt the cloud computing technology for storage. This paper deals with the two important categories of issues on cloud such as traditional issues mostly on web services and other concerned with the implementation of technology such as Service level agreement ,cloud service model ,cloud deployment model. This paper also study about the multilevel integrated cloud security in contrast to famous security-as-a-service concept.

Arti Ochani, Nilima Dongre [6] "Security Issues in Cloud Computing", International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017, proposed the impacts of security on cloud computing and 3rd party control has been examined on the fundamental issues on security. It discusses the issues related to confidentiality, integrity, availability, trust and audit and compliance. This paper also gives brief introduction about the Homomorphic encryption. Different issues related to the service model of cloud are also discuses in this paper. It had also provided the secure cloud computing model which helps in identification of attacks and provides necessary requirements to overcome from the issues.

Dr. Pradeep Kumar Sharma,Prof.(Dr) Prem Shankar Kaushik, Prerna Agarwal, Payal Jain, Shivangi Agarwal, Kamlesh Dixit [7], "Issue and challenges of Data Security In a cloud computing Environment",discussed that with the emergence of cloud computing, Security issues are also increasing. Various attacks on cloud such as attack of an unauthorized access or unwanted activity from outside and inside of cloud can occur due to the storage facilities provided by cloud. It has also incorporated many risks of security such as confidentiality, Integrity, Availability and non-repudiation. This paper discuss about the methods to reduce such risks. It is mandatory to focus on the strategies to make the cloud more secure and user friendly. Thus Instead of focusing on how data is stored. It is much beneficial for an organization to focus on its core business. In order to make the cloud a secure window access for all the employees, it is much important to provide flexibility, scalability and a user friendly environment.

Dr.P.Dinadayalan1, S.Jegadeeswari2, Dr.D.Gnanambigai3 [8], "Data Security Issues in Cloud Environment and Solutions", World Congress on Computing and Communication Technologies, IEEE, 2014.This paper tells about the basic problem in cloud computing related to the security and privacy of data. This paper discusses about the data security issues and their security principles. It also discuss about the need to secure data in cloud computing. Paper tells about the recent researches about it and their possible solution. Cloud technologies, if used appropriately, can help to reduce cost, reduce management responsibilities, increase agility and efficiency of organizations [24].

DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan [9] , "Study on Data Security Policy Based On Cloud Storage", IESEE, 2017. This paper tells about the security issues and related data security policies and how to overcome that issues. In this security risk analysis is done based on the users data stored in cloud. This paper had explained the study of different papers related to security issues. It had also analyzed about Security Strategy of User Data Storage in Cloud Storage.

E. Poornima’, N.Kasiviswanath’, C.Shoba Bindu,[10] ”Key Security Issues and Existing Solutions in Cloud Computing”, Indian journal Of Science and Technology Vol10(19),DOI:10.17485/ijst/2017/V10i19/111016,May2017.This paper offers a brief discussion about the cloud computing and its service models. Also offers a broad discussion about the key security issues and existing solutions at service models of cloud and briefly explains about the security attacks with regard to deployment model and deals with identifying, analyzing, organizing and managing them for security concerns. Major concern of this paper focus on security barriers in adoption of Cloud Computing because of three broad reasons i.e. loss of control of data which is the biggest hurdle in Cloud, lack of trust which is generated by the discern service levels. Thus all three hurdles need to be cured to make the Cloud applications more secure and reliable.

S.Rajeswari, R.Kalaiselvi [11] “Survey of Data and Storage Security in Cloud Computing”, IEEE 2017.This paper provides a wide survey of data and storage security challenges, privacy preservation issues in cloud computing. The security of data is concerned with integrity, authentication, confidentiality which has been further analyzed. The comparison table shows strength and weakness of different approaches that has been studied. Work on access control, data integrity and attribute based encryption has been further analyzed in terms on data security. Each of these works has been studied separately providing detail knowledge about each category.

III. COMPARISON OF EXISTING WORK

A comparative study is shown in below table 1, which talks about the techniques used, privacy, confidentiality, integrity, access control, and storage security from 11 different research paper works by different authors [11].

Table 1: Comparison of Existing Works Based on Data Security in Cloud Computing

Authors	Method	Techniques	Privacy	Confidentiality	Integrity	Access Control	Storage Security
Rachna Jain, Sushila Madan,Bindu Garg	Homomorphic Framework to Ensure Data Security in Cloud Environment	Homomorphic Encryption	Yes	Yes	No	No	Yes
Khalid el makkaoul ,Abdellah ezzati, Abderrahim beni hssane	Challenges of Using Homomorphic Encryption to Secure Cloud Computing	The multi-agent system (MAS)	Yes	Yes	No	Yes	Yes
Prachi Garg ,Dr.Sandeep Goel,Dr.Avinash Sharma	Security Techniques for Cloud Computing Environment	AES and DES Encryption	Yes	Yes	Yes	No	No
Akshay Nayak, Sridhar.N.K, poornima.G.R Dr.Shivashankar	Security Issues in Cloud Computing and its Counter measure	Threat Protection System Using Self-Destructive Mechanism, A Highly Effective Security Model using OTP with help of SMS	No	No	No	No	No
Naim Ahmad	Cloud Computing: Technology, Security Issues and Solutions	Solutions given by CSA and OWASP	Yes	No	No	Yes	No
Arti Ochani, Nilima	Security Issues in Cloud Computing	Secure Cloud	No	Yes	Yes	Yes	No

Dongre		Computing Model using Virtual Private Network (VPN) and cloud service administration					
Prof.(Dr) Pradeep Kumar Sharma,Prof.(Dr) Prem Shankar Kaushik, Prerna Agarwal, Payal Jain, Shivangi Agarwal, Kamlesh Dixit	Issue and challenges of Data Security In a cloud computing Environment	Homomorphic Encryption, Searchable/ structured encryption, Proofs of storage, Server aided secure computation	Yes	Yes	Yes	No	Yes
Dr.P.Dinadayalan1,S.Jegadeeswari2, Dr.D.Gnanambigai3	Data Security Issues in Cloud Environment and Solutions	Solutions based on security principles	Yes	No	No	No	No
DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan	Study on Data Security Policy Based On Cloud Storage	Approach based on the structural characteristics of cloud Storage system.	No	No	No	No	Yes
E.Poornima', N.Kasiviswanath	Key Security Issues and Existing Solutions in Cloud Computing	Local host authentication mechanism, encryption schemes etc	Yes	No	No	Yes	No
S.Rajeswari, R.kalaiselvi	Survey of Data and Storage Security in Cloud Computing	-	-	-	-	-	-

IV. HOMOMORPHIC ENCRYPTION AND ITS CHALLENGES IN CLOUD COMPUTING

The major obstacle over cloud is that confidential data will be used by other enterprises [1]. For that obstacle to overcome or for strengthen the confidentiality of data, we use Homomorphic Encryption technique which is able to perform operation on encrypted data without knowing the secret key, so that data will never be clear neither during transmission nor during processing. In this way it helps in preserving confidentiality and invisibility of the data.

The principles of operations of homomorphic encryption are as follows [19]:

1. Key generation: The client generates the public key (pk) and the secret key (sk).
2. Encryption: The client encrypts the data with encryption key. And sends the encrypted data and public key to the cloud.
3. Storage: The encrypted data and public key are stored in the cloud database.
4. Request: The client sends a request to the server to perform operations on encrypted data.
5. Evaluation: The processing server processes the request and performs the operations by the client.
6. Response: Cloud provider returns to the client the processed result.
7. Decryption: The client decrypts the returned result, using secret key.

A) Fully Homomorphic Encryption

Table 2: Comparison of fully Homomorphic schemes

SCHEMES	ADD. HOMO	MULTI HOMO	MIXED HOMO	APPLICATION
EHES	No	No	Yes	Efficient secure message transmission in mobile Ad hoc Networks
AHEF	No	No	Yes	Applied to perform various calculations on encrypted data
AHEE	No	No	Yes	Secure multi-party computation, electronic voting and mobile cipher

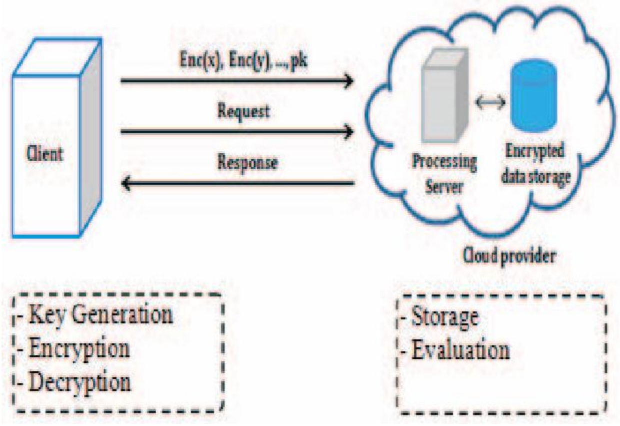

Fig 1. HE Function[19]

We distinguish three categories of homomorphic encryption, depending on the operations performed on the data:

I. Partially Homomorphic Encryption (PHE) [19]: It allows to perform only one operation on encrypted data be it multiplication or addition.

II. Somewhat Homomorphic Encryption (SWHE) [19]: It allows performing more than one operation, but a limited number of multiplication and addition operations.

III. Fully Homomorphic Encryption (FHE) [19]: This is a cryptographic system that supports an unlimited number of both additions and multiplications.

For preserving the confidentiality of the storage, we adopt Homomorphic Encryption technique. But while adopting the Homomorphic Encryption technique, we may face numerous challenges which can surely affect the performance of the Homomorphic Encryption Systems.

A) Efficiency
For a system to be effective, must have the ability to perform more than one type of operations but most partial homomorphic encryption algorithms (RSA, ElGamel, Paillier...) support only one type of operation and as a result these algorithms are restricted from being used in practical applications [19].

B) Robustness
Secondly the robustness can be a big challenge, as robustness of Homomorphic Encryption systems depends on size of encryption key, the large size of public key makes the system too slow for practical use [19].

C) Delay
The choice of the large-size of public key helps ensure the robustness of Homomorphic Encryption systems, on one hand; but on the other hand, they affect the size of ciphertext, the encryption and decryption time, and the data processing time [19].

V. COMPARISON OF VARIOUS HOMOMORPHIC ENCRYPTION SCHEMES

B) Partially Homomorphic Encryption

Table 3: Comparison of Partially Homomorphic schemes

SCHEME	ADD. HOMO	MULTI. HOMO	MIXED HOMO	APPLICATION
RSA	No	Yes	No	To secure internet, Banking &Credit card transaction
ElGamel	No	Yes	No	In hybrid system
Paillier	Yes	No	No	e-voting systems

VI. CONCLUSION

This paper covers overview of the cloud computing and different security related to cloud. Cloud related security issues and their measures are also discussed here. As we know, cloud is tremendously growing technology and everyone is shifting their organisation on to it so security measures are essential components. This paper also discuss about the Homomorphic encryption for security of cloud. Paper also compares different security issues and their counter measures. Literature survey of different security issues and Homomorphic encryption had been explained shortly in it. If the security issues are solved, more number of people will used this widely developed technology without any risk. This paper will help the applicant to analysis the different issues on cloud and how to overcome those issues and whether to use the cloud services or not.

REFERENCES

[1]Akshay Nayak, Sridhar. N.K, poornima. G.R, Dr. Shivashankar, “Security Issues in Cloud Computing and its Counter measure”, 2nd IEEE International Conference on Recent Trends in Electronics Information Communication Technology, May 19-20, 2017, India.

[2] Prof. (Dr.) Pradeep Kumar Sharma, Prof. (Dr.) Prem Shankar Kaushik, Prerna Agarwal, Payal Jain, Shivangi Agarwal, Kamlesh Dixit, “Issues And Challenges of Data Security In A Cloud Computing Environment”, IEEE International Conference,2017,Rajasthan,India.

[3] Naim Ahmad, “Cloud Computing: Technology, Security Issues and Solutions”, IEEE International conference, 2017, Abha, Kingdom of Saudi Arabia.

[4] Akshita Bhandari,Ashutosh Gupta, Debasis Das, “A framework for Data Security and Storage in Cloud Computing” , International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),2016.

[5] Kanagavalli Rangasami, Vagdevi S, “Comparative Study of Homomorphic Encryption Methods for Secured Data Operations in Cloud Computing”, International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2017.

[6] Babitha.M.P, K.R.Remesh Babu, “Secure Cloud Storage Using AES Encryption”, International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016; International Institute of Information Technology (I²IT), Pune.

[7] Anil Barnwal, Satyakam Pugla, Rajesh Jangade, “Various Security Threats and Their Solutions In Cloud Computing”, International Conference on Computing, Communication and Automation (ICCCA), 2017.

[8] Srijita Basu,Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar, “Cloud Computing Security Challenges & Solutions-A Survey”, IEEE International conference, 2018, Kolkata, India.

[9] Meena Kumari, Rajender Nath , “Security Concerns and Countermeasures in Cloud Computing Paradigm”, Fifth International Conference on Advanced Computing & Communication Technologies,2015, Haryana, India.

[10] Zachariah Pabi Gariba, John Andrew Van Der Poll, “Security failure trends of cloud computing”,IEEE 3rd International Conference on Collaboration and Internet Computing, 2017, South Africa.

[11] Arti Ochani, Nilima Dongre, “Security Issues in Cloud Computing”, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.

[12] Papri Ghosh, Vishal Thakor, Dr. Pravin Bhathawala, “ Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms”,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 5, May 20

[13] Garima Gupta, P.R.Laxmi and Shubhanjali Sharma, “A Survey on Cloud Security Issues and Techniques”, Department of Computer Engineering, Government Engineering College, Ajmer.

[14] Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, Rutvij H. Jhaveri, “Survey of Various Homomorphic Encryption algorithms and Schemes”, International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014.

[15] Siddhi Khamitkar, “A survey on Fully Homomorphic Encryption”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. III (Nov – Dec. 2015), PP 10-14.

[16] Wg Cdr Nimit Kaura ,Lt Col Abhishek Lal , “Survey Paper On Cloud Computing Security”, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) ,2017,pune,India.

[17] Jian Li1, Sicong Chen, Danjie Song, “Security structure of cloud storage based on homomorphic encryption scheme”, IEEE CCIS, 2012, China.

[18] M. Ogburn, C. Turner, P. Dahal, “Homomorphic Encryption” In Complex Adaptive Systems, Publication 3, Cihan H. Dagli, Editor in Chief Conference Organized by Missouri University of Science and Technology 2013 - Baltimore, MD, Elsevier, 2013, pp. 502 – 509.

[19] Khalid el makkaoul, Abdellah ezzati, Abderrahim beni hssane, "Challenges of Using Homomorphic Encryption to Secure Cloud Computing" IEEE@2015.

[20]Rachna Jain, Sushila Madan, Bindu Garg, "Homomorphic Framework to Ensure Data Security in Cloud Environment ", 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)

[21] Payal V. Parmar ,Shraddha B.Parmar, Shafika N.Patel, Niyatee I. Bhatt , Rutvij H. Jhaveri ,"Survey of Various Homomorphic Encryption algorithms and Schemes ",International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014

[22] 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

[23] Prachi Garg ,Dr,Sandeep Goel, Dr.Avinash Sharma, "Security Techniques for Cloud Computing Environment ",International Conference on Computing, Communication and Automation (ICCCA2017)

[24] Dr. P. Dinadayalan1, S. Jegadeeswari2, Dr. D. Gnanambigai3, “Data Security Issues in Cloud Environment and Solutions”, World Congress on Computing and Communication Technologies, IEEE, 2014.

[25] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan , “Study on Data Security Policy Based On Cloud Storage”, IEEE 3rd International Conference on Big Data Security on Cloud, 2017.

[26] S.Rajeswari, R.kalaiselvi ,“Survey of Data and Storage Security in Cloud Computing”, International Conference on Circuits and Systems (ICCS 2017), IEEE 2017.

[27] E. Poornima’, N.Kasiviswanath’, C.Shoba Bindu, “Key Security Issues and Existing Solutions in Cloud Computing”, Indian journal Of Science and Technology Vol10(19),DOI:10.17485/ijst/2017/V10i19/111016,May2017.