2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia

Adopting Information Security Techniques for Cloud Computing–A Survey

Tahira Mahboob, Maryam Zahid, Gulnoor Ahmad
Department of Software Engineering
Fatima Jinnah Women University
The Mall, Rawalpindi, Pakistan

***Abstract*—Cloud Computing is widely used technique for data storage on-demand but involves risk such as data security, privacy protection, access-control and data confidentiality. Present study is a survey of the popularly used encryption techniques that is helpful to secure sensitive information on cloud. A discussion of the fundamental challenges and issues/characteristics of cloud computing has been done.Identification of security and privacy issues within this framework are highlighted. Study of the widely used encryption techniques helpful in securing sensitive information on cloud is debated. Scope has been set for academicians and researchers. Diverse versions of the encryption techniques surveyed and analyzed to identify optimization features for cloud security.**

***Keywords* — Cloud Computing; cloud security; data privacy; encryption techniques.**

I. INTRODUCTION

Cloud computing emerges as a computational model on internet as well as distribution design. Its main goal is secure and quick data storage for sensitive information. Cloud computing supports ubiquitous, appropriate, network access to a united pool of resources i.e. servers, storage, networks, services and applications[1]. Now Cloud computing has become a point of attention in the scientific and industrial group of communities. Cloud computing have an ability to enhance scalability, availability, reliability etc. Cloud computing provides compelling benefits towards the society but there are also a factor of risk i.e. data security and privacy protection of sensitive data, authentication of user, access control, application security[2]. Many organizations shift their personal data on the cloud but large organization still hesitate migrating to cloud due to security concerns.

Present study is poised as a survey to explore the encryption techniques to resolve the security issues on cloud computing. Diverse versions of the encryption techniques were surveyed and analyzed to identify optimization features for cloud security. Paper focuses on different criteria that effect the security of cloud and propose encryption technique to resolve it. Data security is among the challenges that will increase great concerns for the user when a person stores sensitive information on the cloud servers. The origin of these concerns are that cloud servers; generally operated by commercial providers do not meet the trusted domain of the users.

Three major concerns are involve within the cloud computing:

- Move the personal sensitive data to the cloud servers.
- Move data from cloud servers to the client's or customer's computer and
- To store customer's personal information in cloud server is known as remote server (not owned by the customers).

II. LITERATURE REVIEW

Amlan jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim and Hoon Jae Lee[3], focused on security user authentication issue. This paper proposed the strong two-step user authentication process where user is verified before enter into the cloud. Even user can change his/her password whenever it is required. This technique restrict many attacks like denial of service and it provide efficiency to cloud computing. Hongwei Li, Yuanshun Dai1, Ling Tian, and Haomiao Yang[4], focused on authentication issue, which is important for both users and services. This paper proposed Identity-based authentication of cloud computing and it services combination of Identity-based Hierarchical Model and corresponding encryption and signature. After simulation, it is conclude that it protocol is more efficient and lightweight than other protocols.

Ari Juels, Alina opera[5], proposed the framework that secure cloud data by integrity and verification for data availability. Major obstacle in cloud computing is to obtained security and operational risks i.e. hardware failure, malware, software bugs etc. So, protected for outsourced data on cloud is necessary. There is also another issue in public clouds is availability and reliability assurances. Mariana Carroll, Alta van der Merwe and Paula Kotzé[6], focused easing for cloud security risk as a compulsory step to ensure secure cloud environment. It provided an overview about the cloud computing security risks i.e. attention to ensure about integrity, completeness and availability of data as well as benefits that helps to build standards, processes and controls includes data security, logical access, network security, physical security and compliance.

Deyan Chen and Hong Zhao[7], analyzes the data security and privacy protection issues in cloud computing. Because of these issues, many large organization still don't share their data on cloud. Privacy protection is shared data

with protecting personal information. The most fundamental challenges are access control and separation of sensitive data. This paper proposed different techniques to ensure access i.e. fine-grained access authorization.

Nirmala, R. K. Shivanadhan and R. Shanmuga Lakshami[8] focused the inactive information's arrangement security is to be done by encoding the information or data and send it to server that's how confidentiality and integrity of data is implemented by encoding the data. Further the general idea of distinguishing security issues that influences the cloud environment and related work that are did in the territory of truthfulness are discussed.

Kaaniche, N.; Boudguiga, A.; Laurent, M.[9], proposes a cryptographic plan for secure management of data by using the ID based cryptography[4]. This is done by encoding the information which are too kept in open server and it is also done by getting the information and sharing it among clients so that unauthorized client cannot get the information without the owner permission.

Advantage of such act is to have data access to only approved customers or owners as presented by Arockiam, L.; Monikandan, S. [10]. Encryption with obscurity; both concepts are exclusive for securing information in storage management. Obstruction is process which masquerades unauthorized clients by implementing an exact numerical capacity or utilizing programming techniques. Encryption is the procedure of changing over the comprehensible content into mixed up structure utilizing a calculation and a key. Disorder is same like encryption. Applying encryption and muddling systems on the cloud information will give more assurance against unapproved usage of data.

Kavuri, S.K.S.V.A.; Kancherla, G.R.; Bobba, B.R.[11] presented that focused information can be gained by client. Such as reports, media or other sort of proofs utilizing outsider produced validation key. For reducing the security issues of cloud computing servers; advance message based confirmation process is defined. It is the process only approved users can have access to data by identifying his/her identity using message uprightness.

Zhang Jianhong; Chen Hua [12], focused cloud computing data storage security requires new techniques. The issue of promising the information security is discuss furthermore another decency check plan is proposed that is RSA security possibility. Advantage of this approach or technique is that the customer don't have to keep copy of data with him somewhere else all data will save in clod computing.

Kaur, R.; Singh, R.P. [13], discussed to secure the level of distributed storage security a security model is proposed having three stages private, public, and hybrid. Some encryption techniques are implemented on these three stages to cover areas regarding security factor. Two tier security structural arrangement for hybrid. Decoding and encryption techniques for public stage and last the exclusive token era instrument is implemented for private stage. All these gives and advantage of enhancing security, integrity in cloud computing.

Zhuo Tang,Juan Wei,Ahmed Sallam,Kenli Li,Ruixuan L.[14], proposed another access control in view of Role-based access control (RBAC) model. This model incorporates two sort of parts, client part (UR) and proprietor part (OR); such that, Users get qualification from proprietors to correspond with administration supplier and to get access authorizations of assets.

Rajani Kanth Aluvalu, Lakshmi Mundane [15], Privacy, trust, access control are the key factor for maintaining security in cloud computing. Distributed computing have many benefits regarding sharing data among untrusted users. Granularity of access control with a successful encryption technique are explained and discussed. Furthermore different access control models for disseminated computing are examined.

Wayne A. Jansen[16], explored key issues, which had long-term importance in cloud hooks (security and privacy issues). The idea of the requisite can be scaled up or down on the need of the assets. IT now-a-days are using cloud computing models. Security of cloud computing greatly depends on the cryptography.

Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou [17], proposed a hybrid technique i.e. attribute-based encryption, proxy encryption and lazy re-encryption. Keeping the customer or user confidentiality the most broadly utilized process is encryption. Encryption only is not that powerful to secure data to have more security paper proposes encryption with obscurity. These hybrid method, after analysis, proved to be highly efficient and secure. This technique is highly useful against fine-grained data access control.

III. ANALYSIS

To control data and access to data multi-tasking is done in cloud computing. Constructing secure platform for any data combining different encryption techniques for data integrity, confidentiality and availability is a good scheme and in this paper, different papers are surveyed to find better techniques for data security in cloud computing.
Parameters for analysis are selected and are limited by the scope of the research papers under study. Total 12 parameters have been chosen and analysis is carried out based on them as represented in Table I. Analysis is represented in Table II and the graphical analysis on basis of the selected parameters in presented in the fig. 1.

Amlanjyoti Choudhary,[3][15] alongwith other authors showed concern about user authentication by proposing authentication techniques to enter in cloud. For maintaining, data confidentiality is a challenging issue because it is difficult to control data access from unauthorized users [9]. Author[4] suggested methodology for data confidentiality using encryption techniques for better security of data of data owners. Cloud computing

allows valid users to have access of resources and information as many malevolent attackers can also try to access the data and solution to this problem is data integrity and privacy so that accessing the information should be difficult for invalid users and this work is suggested by Ari Juels in 2013[5].

On the conclusion of the research survey and analysis it is determined that the Data security techniques, authentication algorithms adopted and the Methodology implemented for is of principal concern whenever designing a cloud computing environment/network.

TABLE I: EVALUATION CRITERIA FOR SECURITY OF THE CLOUD COMPUTING: A SURVEY

Evaluation Parameters	Meaning	Possible Values
User Authentication	Confirming the access of data to authorized user.	Yes, No
Data Confidentiality	Rule that promise the access of patent's data.	Yes, No
Privacy protection	Proposed technique gives user a privacy or not.	Yes, No
Data Security	System is secure or not	Yes, No
Non-repudiation	The declaration that somebody cannot refuse something.	Yes, No
Data Integrity	The quality of being whole.	Yes, No
Availability of data and services	Data available to any specific user.	Yes, No
Data Control	Data hosted by some services provider.	Yes, No
Access control	Data access by some encryption technique.	Yes, No
Methodology	Specific method used.	Yes, No
Data encryption	Data secured by some key that is shared.	Yes, No
Efficiency	System is efficiency in term of working speed, error free.	Yes, No

TABLE II: ANALYSIS OF PARAMETERS FOR SECURITY OF THE CLOUD COMPUTING: A SURVEY

Sr.	Authors/ Parameters	User authentication	Data Confidentiality	Privacy Protection	Data Security	Non-repudiation	Data Integrity	Data Availability	Data Control	Access Control	Methodology	Data Encryption	Efficiency
1	Amlanjyoti Choudhury,2011	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No	No	Yes
2	Hongwei Li1,2009	Yes	Yes	No	Yes	No	No	Yes	No	No	Yes	Yes	Yes
3	Ari Juels,2013	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No
4	Mariana Carroll,2011	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
5	Deyan Chen,2012	No	Yes	Yes	Yes	No	No	No	No	Yes	No	No	No
6	V. Nirmala	Yes	Yes	No	Yes	No	Yes	No	No	Yes	Yes	Yes	No
7	Kaaniche, 2013	Yes	Yes	No	Yes	No	No	Yes	No	No	Yes	Yes	Yes
8	Arockiam, L.,2014	No	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes
9	Kavuri, S.K.S.V.A.,2014	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No
10	Zhang Jianhong, 2010	Yes	No	No	Yes	Yes	Yes	No	No	Yes	Yes	No	No
11	Kaur, R.,2014	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
12	Zhuo Tang, 2012	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	No	No
13	Rajani Kanth Aluvalu, 2015	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
14	Wayne A. Jansen,2011	No	Yes	Yes	Yes	No	Yes	yes	Yes	Yes	No	Yes	No
15	Shucheng Yu,2010	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes

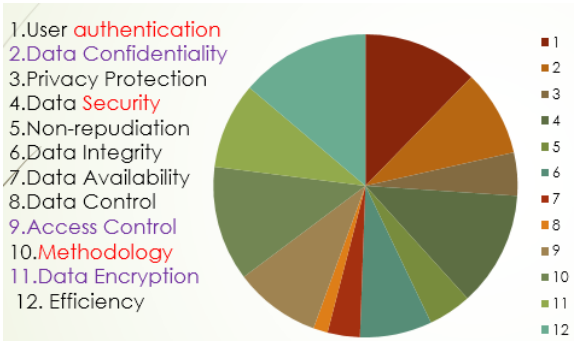

Fig 1. Graphical Representation of Analysis Parameters

IV. CONCLUSION

The structural design of cloud computing intimidates the security of data due to some techniques and user have problems regarding their data to be uploaded. As cloud computing providing compelling benefits towards the society but on the other hand, there are also a factor of risk i.e. data security and privacy protection of sensitive data, authentication of user, access control, application security. It main goal a secure and quick data storage for sensitive information.

This survey is explicitly regarding the techniques that are discussed in different papers to secure data, to have confidentiality of data, integrity of data. User authentication and control access is still a highlighted factor in cloud computing. Basically for any organization the thing that matter is security of data. To keep data save from any hacking because of sensitive and important data. Data hacking is now become very common. Therefore, data confidentiality is an important feature of cloud computing. So to secure them encryption techniques are discussed in this study as day by day technology is becoming advance and data is needed to be secure. Encryption only is not that powerful to secure data to have more security paper proposes encryption with obscurity.

Main focus of the researchers in connection to cloud computing is authentication, security and the methodology adopted followed by the confidentiality, access control and data encryption. To secure them encryption techniques are discussed in this paper as day by day technology is becoming advance and data is needed to be secure. Encryption only is not that powerful to secure data to have more security paper proposes encryption with obscurity.

FUTURE WORK

After analysis, the main reason that large organization still not move their sensitive information to cloud is its security issue. This security problem can be resolve by applying different encryption techniques to cloud computing. Confusion and diffusion need to be kept strong when choosing the encryption techniques.So that, organization/ enterprises transfer their important data on cloud.

ACKNOWLEDGMENT

This research paper is made possible through the help and support by our instructor Ms. Tahira Mahboob, Fatima Jinnah Women University, Rawalpindi, Pakistan. Any findings, analysis and conclusion or future work expressed in this material are those of the authors and our instructor.

REFERENCES

[1] Mell, P., and Grance, T. (2011). The NIST definition of cloud computing.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A. and Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[3] Amlan jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim and Hoon Jae Lee, *"*A Strong User Authentication Framework for Cloud Computing*", IEEE Pacific services Computing Conference*, 2011

[4] Hongwei Li1, Yuanshun Dai1,2, Ling Tian1, and Haomiao Yang, *"* Identity-based Authentication for Cloud Computing*"*, *Springer- Verlag Berlin Heidelberg*, 2009.

[5] Ari Juels, Alina opera, "New Approaches to Security and Availability to Cloud Computing*", ACM-RSA laboratories*, 2013.

[6] Mariana Carroll, Alta van der Merwe and Paula Kotzé, "Secure Cloud Computing Benefits, Risks and Controls*"*, *IEEE-Information Security South Africa*, 2011.

[7] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", *IEEE-Conference on computer science and electronic engineering,* 2012.

[8] V. Nirmala, R. K. Shivanadhan and R. Shanmuga Lakshami , "Data Confidentiality and Integrity Verification using User Authenticator scheme in Cloud" , *International Conference on Green High Performance Computing, IEEE* , pp.1 -5

[9] S Kamara, K Lauter, "Cryptographic Cloud Storage", IFCA/LNCS 6054, *Springer-verlag, Berlin Heidelberg*, 2010, pp 136-149.

[10] Arockiam, L.; Monikandan, S., "Efficient cloud storage confidentiality to ensure data security," *Conference in Computer Communication and Informatics (ICCCI), IEEE*, vol., no., pp.1-5, 3-5 Jan 2014.

[11] Kavuri, S.K.S.V.A.; Kancherla, G.R.; Bobba, B.R., "Data authentication and integrity verification techniques for trusted/untrusted cloud servers," *Conference in Advances in Computing, Communications and Informatics* (ICACCI, IEEE, vol., no.,pp.2590-2596, 24-27 Sept. 2014

[12] Zhang Jianhong; Chen Hua, "Security storage in the Cloud Computing: A RSA-based assumption data integrity check without original data," *Conference in Educational and Information Technology (ICEIT), IEEE,* vol.2, no., pp.V2-143-V2-147, 17-19 Sept 2010.

[13] Kaur, R.; Singh, R.P., "Enhanced cloud computing security and integrity verification via novel encryption techniques," *International Conference in Advances in Computing, Communications and Informatics (ICACCI), IEEE*, vol., no., pp.1227-1233, 24-27 Sept. 2-14.

[14] Zhuo Tang,Juan Wei,Ahmed Sallam,Kenli Li,Ruixuan L "A new RBAC based access control model for cloud computing" GPC'12 Proceedings of the 7th international conference on Advances in Grid and Pervasive Computing.Pages 279-288 Springer-Verlag Berlin, Heidelberg 2012.

[15] Aluvalu, R., & Muddana, L. (2015). A Survey on Access Control Models in Cloud Computing. In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1 (pp. 653-664). Springer International Publishing.

[16] Wayne A. Jensen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", IEEE- 44th Hawaii conference on System Science, 2011.

[17] Shuchend Yu., Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE-INFOCOM, 2010.