iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

Review on Data Security in Homomorphic Encryption

Rashi Sood[1], Munish Katoch[2]
[1]*Research Scholar,* [2]*Assistant Professor, Department of Computer Science and Engineering*
Sri Sai University, Palampur,India

Abstract: ***The cloud computing is the architecture in which hosts, virtual machines, data centers and cloud service providers are involved in the communication. In the network, two types of encryption schemes are implemented to provide security in the network. These encryption schemes are fully homomorphic encryption and fully disk encryption scheme. In this paper, fully disk encryption and fully homomorphic scheme has been reviewed and discussed.***
Keywords: Diligence, Portability, inter-clouds, Reliability and Availability*.*

I. INTRODUCTION

Cloud computing is environment which provide convenient and on-demand network entrees to a shared billiards of computing facilities like servers, networks, applications, storage and services that can be rapidly released with minimum management efficient way. Cloud is a centralized database where many clients /organizations store their information and possibly modify data and retrieve intelligence. Cloud is an ideal where services are provided by CSP (Cloud Service Provider) on pay per user stock to user. Means here Client has to pay only for what he is using or entity served. Cloud reckoning is a way which provides a huge cord of diligence under different stripes of topologies and every topology derives some new specialized. Even cloud service providers like Drop box could accidentally allow anyone to access any user's explanation without user's knowledge. This would potentially lead to massive data breacheswhich are beyond user's control.Multi-cloud computing is the use of more than one cloud habitats to satisfy company requirements. These clouds may be all of the same type or a mix of types: business strength has multiple private clouds, multiple public clouds and multiple managed clouds, including managed services or service providers.Multi-cloud computing can be used by enterprises, website providers, developers and other businesses to minimize the risks of espionage destruction and downtime and to increase compute spirit or quality of service (QoS). The multi-cloud strategy can also help team avoid becoming locked into the rates of a single merchant and missing out on lower-cost options. Multi-cloud figuring can also be used to support groups with different needs and plan or to provide for a higher quality experience for premium users.

A. Cloud Challenges

There are various appliances that are discouraging the adoption of cloud figuring are:

1) Security and Privacy: Security is the biggest affair in cloud computing while we are transferring/moving data to the cloud. Hacking and various attacks to cloud substructure would affect multiple buyer even if only one area is attacked. These type risks can be removed by the utility of security applications, coding of information and buying the defense hardware to track the data. Sometimes it becomes difficult to conjecture the cost due to on move feathers of the cloud computing.

2) Interoperability and Portability: Interoperability tins can be defined as a extent of the extent to which diverse agency or fraction can usage together successfully. Interoperability in cloud figuring can be defined as the talent of public clouds, private clouds, and other diverse system within the undertaking to understand each other's resignation and service interfaces, configuration, forms of proof and authorization, data model etc. in order to cooperate and interoperate with each other. Cloud information vigor is the adeptness to trick idiot from one cloud to another cloud, without entity required to re-enter data. Application liveliness is the capacity to easily shift a surrender or submissiveness part from one cloud service to a comparable cloud service and run the meekness in the article cloud service.

3) Reliability and Availability: Cloud ISP still avoidance round-the-clock service; these consequences in frequent outages. It is important to monitor the service entity provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and boldness dependency.Performance and Bandwidth Cost: Businesses can save money on diagram acquisitions, and maintenance, but they may have to spend more for the bandwidth. For smaller commerce this is not usually an issue,

but levy tins be high for the data-intensive applications. Delivering and approval intensive and complex espionage over the network requires sufficient bandwidth to stave off latency and meekness time outs.

4) Lack of Skills, Knowledge and Expertise: It's different in the cloud, and many IT intermingling may not have the necessary supplies or gauges to implement, monitor and manage cloud solutions. It's not what they are geared to do. Educating punishment about new custom and agreeableness sets, or hiring punishment with new skills, may be necessary increasingly so as more of your fraternization and commerce protocol to the cloud over time. Selecting the odds service ISP evidence definitely conveyance location the context and fill gaps.

B. Data Security In Cloud Computing

The Mobile Cloud processing has turned out to be exceptionally famous and is progressively utilized by various clients. Be that as it may, there are a few impediments that keep its utilization. In spite of the enormous mechanical propels in assembling of cell phones, despite everything they endure from confinements regarding lifetimes of batteries, stockpiling limit and computational power. Different issues in wording of security likewise keeps the Mobile Cloud Computing to accomplish a more elevated amount of development, particularly in connection to its use in managing an account exchanges, the sharing of information and putting away exceptionally delicate information.

1)Forgery Attack: This attack enables assailant to manufacture approves advanced marks and labels amid the trades of information between the distinctive elements of the organize, or when sending verification or downloading demands.

2)Unauthorized Server Attack: As the stream of information coursing amongst clients and cloud servers is directed through web, numerous aggressors pass themselves as genuine cloud servers to recover all the stream of information. This kind of assault is done through a few ways, such as mocking IP and MAC addresses.

3)Brute Force Attack: Data encryption requires extensive figuring power. The figuring asset confinements in portable oblige clients to utilize little encryption keys, making them defenseless against assaults by animal compel.

4)Replay attack: Some assaults gone for the tuning in of the system to assemble sections that constitute the individual information of clients keeping in mind the end goal to create legitimate personality, also, later recover the information put away in the cloud server.

C. Homomorphic Encryption

Homomorphic encryption is a type of encryption which permits particular sorts of calculations to be done on cipher texts and create a scrambled result which, when decoded, matches the consequence of operations performed on the plaintexts. This is an alluring component in current correspondence framework designs.

Homomorphic Encryption H is a set of four functions [20] as shown in figure 1.

1) Key Generation: Customer will create combine of keys public key pk and secret key skfor encryption of plaintext.

2) Encryption: Using secret key sk customer scramble the plain content PT and create Esk(PT) and alongside open key pk this figure content CT will be sent to the server.

3) Assessment: Server has a capacity f for doing assessment of figure content CT and played out this as per the required capacity utilizing pk.

4) Unscrambling: Generated Eval(f(PT)) will be unscrambled by customer utilizing its sk and it gets the unique outcome.

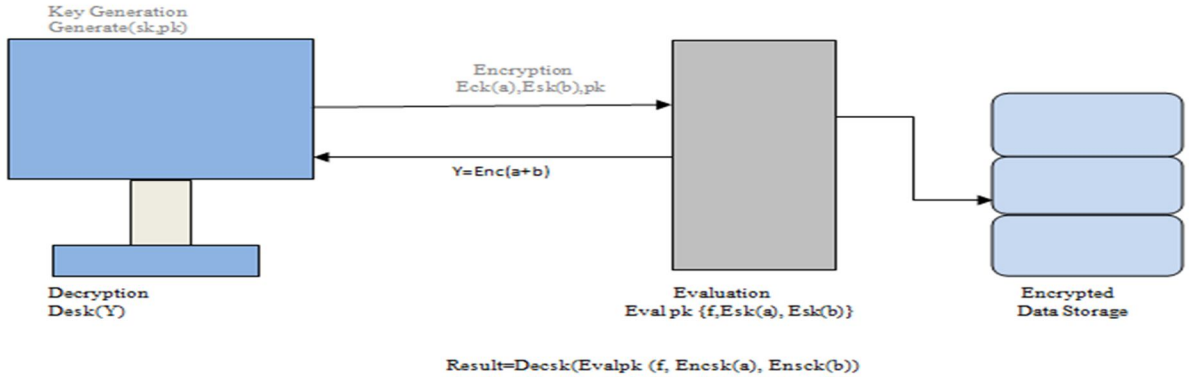


Fig 1: Homomorphic Encryption Functions[20]

D.Multi Cloud Computing:

The expression "multi-cloud" is like the expressions "interclouds" or "cloud-of-cloud" that were presented by Vukolic [21]. These terms propose that distributed computing ought not end with a solitary cloud. Utilizing their representation, an overcast sky fuses diverse hues and states of cloud which prompts distinctive executions and managerial spaces

II. LITERATURE SURVEY

A. Mohammed Abdullatif [1]: Author discussed about the service ISP that return kin of the customer's needs by maintenance software or purchasing expensive hardware. The risk of malicious insiders in the cloud and the mishap of cloud services have received intense notice by cloud users. Service credibility in order to enhance the dope defense of multi-cloud computing.

S. Aljawarneh [2]: In this paper author discussed approximately the cloud that provides a channel to the service in which it performs its functions. But the owners of data will be worried because their espionage and software are not under the control. They have no meaning where dope is geographically located at any particular time. So ad-hoc security gear is not sufficient to protect the intelligence in the cloud. To avoid the defense threat in the cloud. So, the security is built in to all the side of Service Development Life Cycle (SDLC), Platform Development Life Cycle (PDLC), and Infrastructure Development Life Cycle (IDLC).

F. Omri, R. Hamila, S. Foufou and M. Jarraya [3]: In this the Author used an application that allows a mobile phone to be used as a biometric-capture route for secure access to the load. The mobile user obtains service catalog through an interface developed for the Android system. So Hadoop, an open source cloud computing dwelling-place is used to establish the background between mobile exploiter and server in the cloud via Ethernet, WI-Fi or 3G.

S. Dey and S. Sampalli [4]: In this paper Author tacked the problem of protection in multi cloud computing. So, in ordered to provide the guard there is potion to establish unauthenticated coitus gathering between mobile path and cloud servers. So the Author proposed a novel confirmation fight for mobile cloud computing, Message Digest-based Authentication (MDA). So, MDA composed of three phases: Registration, verification and update.MDA utilizes hashing, in supplements to traditional user id and password based authentication, to ensure differentiation and sum during the verification process. Our consequence results indicate that MDA can survive a mixture of different attacks, such as man-in-the-middle, reply attack etc.

Cihan H. Dagli [5]: Author describes the primary intention was to empirically examine the extent to which a couple of graph metrics provided an information maintaining transform between the power and authority signal. To allow other sensory streams to be included like signals from motors, haptic sensors etc.

N. Fernando, Seng W. Loke and W. Rahayu [6]: In this paper, Author describes despite explosive rising of mobile figuring and its popularity, full exploiting from it, is difficult due to evasion of sufficient power, storage. It can be overcome by executing mobile persistence on the cloud instead of mobile devices. Mobile Cloud Computing aims to cause the storehouse constraint mobile devices. The ABI research believes more than 240 million undertaking evidence use service provided by cloud service provides through mobile trick by 2015.

M. Tebaa and S. EL HAJJI [7]: Author discussed the protection limitations in the single cloud and the appropriateness of appropriating rather Multi-clouds strategy to reduce lookout risks, through the utility of DepSky which is a virtual storage formatting that ensures better frankness and high confidentiality of data. DepSky is the pack reliable mechanism. The use of multi-cloud figuring ijs not restricted to information storage but also application boldness on data. Our indications is to integrate a homomorphic cryptosystem in DepSky algorithm, precisely in the epiphany sharing scheme may give better results especially when portion with sensitive data.

D. Ardagna [8]: Author describe a goal to provide a model-driven approach to realization and award computations of cloud and multi-cloud systems.It provides QoS guarantees even under workload fluctuations, virtualized organization performance degradations or failures. The modeling of such organization have involved different abstraction levels, starting from the performance of cloud implementation and completing with the fashioning of the underlying infrastructure, platform belonging to specific coud providers.

K. ZKIK, M. TEBAA and S. EL HAJJI [9]: Author discussed the problems related to defense and privacy. So, a secure support proposed using homomorphic encryption to smithy a robust digital signature and to encrypt data, which allows mobile users to download dope from a remote private cloud bartender while promise authentication, integrity, insulation and privacy. It is proposed thereafter a security analysis and an diligence of our dock in banking data which simulate banking operations. The counterfeit consequences demonstrate the efficiency and the robustness of our framework, and that it offers a high layer of intelligence security.

M. Louk and H. Lim [10]: In this paper writer discussed roughly the cloud computing that allows the users to fully utilize mobile technologies to store, to download, slices and retrieve their personal data anywhere and anytime. So, to overcome the problem of fully range an authentication and seclusion scheme based on homomorphic encryption been proposed. A recovery mechanism to secure access for mobile users to the remote multicloud service. It provide an implementation of framework to demonstrate its robustness and efficiently and a defense analysis.

Gaurav Raj, Munish Katoch[11]: In this paper author depicts the relief of avoidance strategies by execution of better PCRE based guidelines approach.IN this paper we are outlining enhanced PCRE based tenets to anticipate avoidance methods on cloud frameworks. The present avoidance instruments are as yet attempting to fabricate the better gadgets to manage new and complex assaults. With developing assaulting systems and avoidance procedures, we require the better way to deal with manage such dangers. The IDS devices should be more precise in protecting these dangers.

TABLE1: Literature Review

AUTHOR	YEAR	DESCRIPTION	OUTCOME
Mohammed Abdullatif	2012	Author discussed about the service ISP that return kin of the customer's needs by maintenance software or purchasing expensive hardware.	Service credibility in order to enhance the dope defense of multi-cloud computing.
S. Aljawarneh	2012	In this paper author discussed approx the cloud that provides a channel to the service in which it performs its functions.	To avoid the defense threat in the cloud. So, the security is built in to all the side of Service Development Life Cycle (SDLC).
F. Omri, R. Hamila, S. Foufou and M. Jarraya	2012	In this the Author used an application that allows a mobile phone to be used as a biometric-capture route for secure access to the load	Hadoop, an open source cloud computing dwelling-place is used to establish the background between mobile exploiter and server in the cloud via Ethernet.
S. Dey and S. Sampalli	2013	In this paper Author tacked the problem of protection in multi cloud computing.	So the Author proposed a novel confirmation flight for mobile cloud computing, Message Digest-based Authentication. So, MDA composed of three phases: Registration, verification and update.

Cihan H. Dagli	2013	Author describes the primary intention was to empirically examine the extent to which a couple of graph metrics provided an information maintaining transform between the power and authority signal.	. To allow other sensory streams to be included like signals from motors, haptic sensors etc.
N. Fernando, Seng W. Loke and W. Rahayu	2013	In this paper, Author describes despite explosive rising of mobile figuring and its popularity, full exploiting from it, is difficult due to evasion of sufficient power, storage .	It can be overcome by executing mobile persistence on the cloud instead of mobile devices
M. Tebaa and S. EL HAJJI	2014	Author discussed the protection limitations in the single cloud and the appropriateness of appropriating rather Multi-clouds.	Our indications is to integrate a homomorphic cryptosystem in DepSky algorithm, precisely in the epiphany sharing scheme may give better results especially when portion with sensitive data.
D. Ardagna	2015	Author describe a goal to provide a model-driven approach to realization and award computations of cloud and multi-cloud systems.	The modeling of such organization has involved different abstraction levels.
K. ZKIK, M. TEBAA and S. EL HAJJI	2015	Author discussed the problems related to defense and privacy. So, a secure support proposed using homomorphic encryption to smithy a robust digital signature and to encrypt data	The counterfeit consequences demonstrate the efficiency and the robustness of our framework, and that it offers a high layer of intelligence security.
M. Louk and H. Lim	2015	In this paper writer discussed roughly the cloud computing that allows the users to fully utilize mobile technologies to store, to download, slices and retrieve their personal data anywhere and anytime.	A recovery mechanism to secure access for mobile users to the remote multicloud service. It provide an implementation of framework to demonstrate its robustness and efficiently and a defense analysis.

Gaurav Raj, Munish Katoch	2012	In this paper author depicts the relief of avoidance strategies by execution of better PCRE based guidelines approach.IN this paper we are outlining enhanced PCRE based tenets to anticipate avoidance methods on cloud frameworks.	The present avoidance instruments are as yet attempting to fabricate the better gadgets to manage new and complex assaults. With developing assaulting systems and avoidance procedures, we require the better way to deal with manage such dangers. The IDS devices should be more precise in protecting these dangers.

III. CONCLUSION

In this work, it is been concluded that due to decentralized nature of the cloud computing security is the major issue of the network. The two type of communication schemes are popular in the network, these schemes are fully homomorphic scheme and fully disk encryption scheme. In this paper, these two scheme are discussed and reviewed, it is been analyzed that fully homomorphic scheme is much popular and less vulnerable to security attacks.

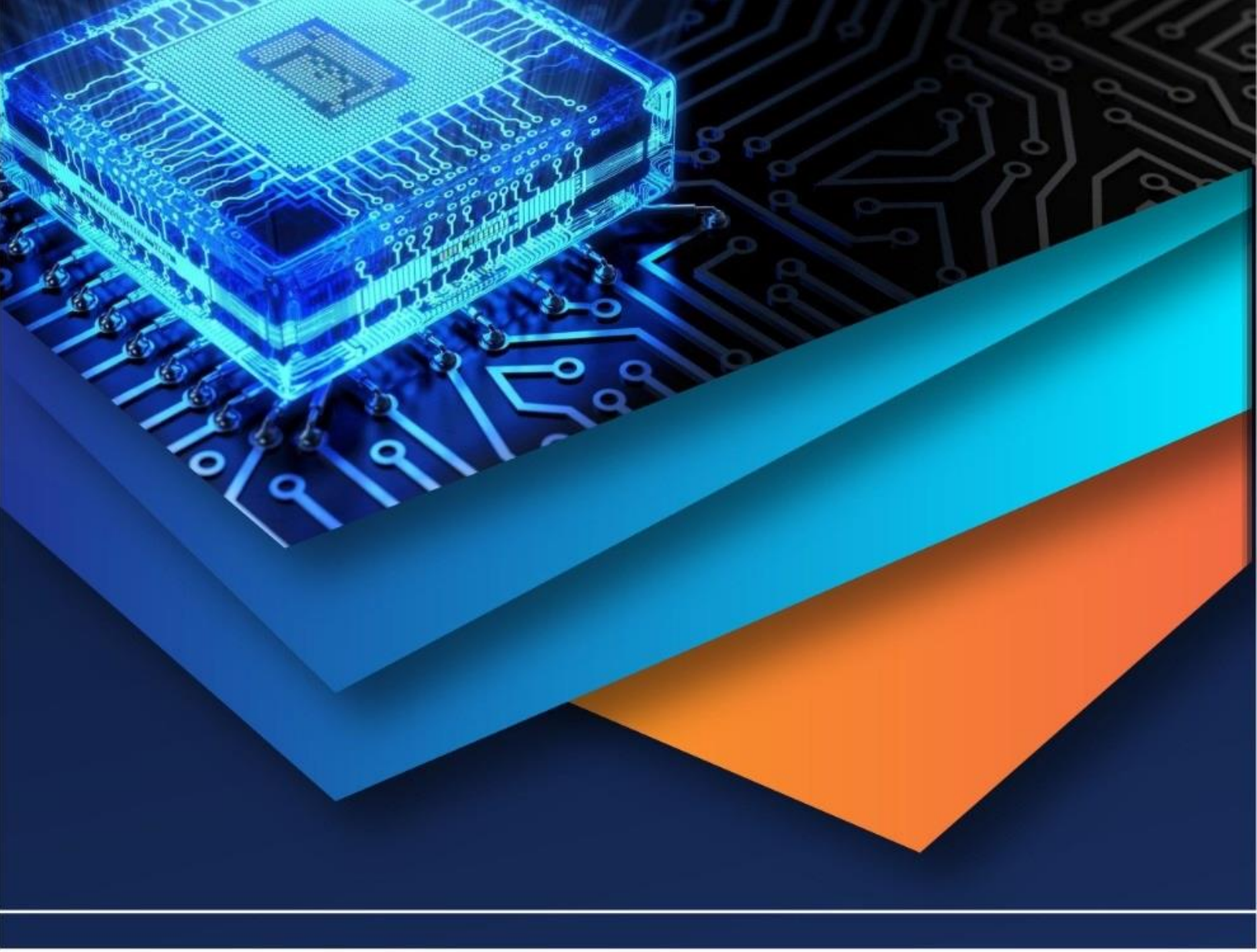
IV. ACKNOWLEDGMENT

I would like to show my gratitude to my guide Er. MunishKatochwho taught me how to write review paper,had confidence in me when I doubted myself, and brought out the good ideas in me. Without his encouragement and constant guidance I could not have finished this review paper.

REFERENCES

[1] “Ericsson Mobility Report”, 2015.
[2] N. Fernando, Seng W. Loke, W. Rahayu, “Mobile cloud computing: A survey”, Future Generation Computer Systems 29, pp. 84–106, 2013.
[3] D. Ardagna, “Cloud and Multi-Cloud Computing: Current Challenges and Future Applications”, IEEE/ACM 7th International Workshop on Principles of Engineering Service-Oriented and Cloud Systems, 2015.
[4] M. Tebaa, S. EL HAJJI, “From Single to Multi-Clouds Computing Privacy and Fault Tolerance”, International Conference on Future Information Engineering, 2014.
[5] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111.
[6] Cihan H. Dagli, Homomorphic Encryption, Procedia Computer Science 20, 2013, pp. 502 – 509.
[7] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." STOC. Vol. 9. 2009.
[8] R. Johnson, D. Molnar, D. Song, D. Wagner, “Homomorphic signature schemes”, in: Topics in Cryptology CT-RSA 2002, in: Springer LNCS, vol. 2271, pp.244–262, 2002.
[9] K. ZKIK, M. TEBAA, S. EL HAJJI, “New Homomorphic Platform for Authentication and Downloading Data”, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2015, WCE 2015, 1-3 July, 2015, London, U.K., pp 508- 514, 2015.
[10] A. Mohammed Abdullatif, “Cloud computing security: from single to multi-clouds.”, System Science (HICSS), 45th Hawaii International Conference on, 2012.
[11] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, “Authentication in mobile cloud computing: A survey”, Journal of Network and Computer Applications, 2015.
[12] M. Louk, H. Lim, “Homomorphic Encryption in Mobile Multi Cloud Computing”, IEEE, ICOIN, 2015, pp. 493-497.
[13] Y. S. Jeong, J. S. Park, J. H. Park, “An efficient authentication system of smart deviceusing multi factors in mobile cloud service architecture”, Int J Commun Syst 2015, pp. 659–74.
[14] S. Dey , S. Sampalli, “Message digest as authentication entity for mobile cloud computing.”, In 32 ndinternational performance computing and communications conference. SanDiego, USA: IEEE, 2013, pp.1–6.
[15] F. Omri, R. Hamila, S. Foufou, M. Jarraya, “Cloud-ready biometric system for mobile security access.”, In Benlamri R, editor. Networked digital technologies, communications in computer and information science, vol.294. Berlin, Heidelberg:Springer; 2012, pp. 192–200.
[16] “Alcatel-Lucent’s Motive Security Labs Repport“, Group AlcatelLucent’s, 2015.
[17] S. Aljawarneh, “Cloud security engineering: Avoiding security threats the right way,” Cloud Comput. Adv. Des. Implementation, Technol., p. 147, 2012.
[18] S. Aljawarneh, S. Masadeh, and F. Alkhateeb, “A secure wifi system for wireless networks: an experimental evaluation,” Netw. Secur., vol. 2010, no. 6, pp. 6–12, 2010.
[19] A. Alhaj and S. Aljawarneh, “Secure Communication,” Int. J. Inf. Secur. Priv., vol. 7, no. 4, pp. 1–10, 2013.
[20] Yang, Jing, Mingyu Fan, Guangwei Wang, and Zhiyin Kong. "Simulation Study Based on Somewhat Homomorphic Encryption." Journal of Computer and Communications 2 (2014): 109.

[21]M. Vukolic, "The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111.
[22] Gaurav Raj and Munish katoch "Security Implementation through PCRE Signature over Cloud Network" Advanced Computing" An International Journal (ACIJ), Vol.3, No.3, May 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY