IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Impact of Asymmetric Encryption in Cloud Computing: A Study

M. Ilakiya[1*], R.Vijithra[2], K. Kuppusamy[3] , J.Mahalakshmi[4]

[1,2,4]Department of Computer Science, Alagappa University, Karaikudi, Tamilnadu, India
[3]Department of Computational Logistics, Alagappa University, Karaikudi, Tamilnadu, India

[*]*Corresponding Author: ilakiyamuruges@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i3.894897 | Available online at: www.ijcseonline.org

Accepted: 21/Mar/2019, Published: 31/Mar/2019

Abstract—"Cloud Computing" a form of On-demand computing used by business peoples, organizations and institutions on pay –as-you basis. The Cloud Computing paradigm have many advantages such as availability, scalability, automated updates on software, enhanced collaboration and easily manageable, that makes it as an efficent medium for use. Security threat to its data stored in shared medium is a major concern. To ensure the authentication of the data many mechanisms were in use. Over past decades Cryptography is one most widely used technique for concealing data from third party. Symmetric key cryptography uses the similar key for both the encryption and decryption of messages. Instead, Asymmetric key cryptography uses two different types of keys. This paper discussed about the brief overview of algorithms and mechanisms done by the researchers regarding authentication and authorization issues in the asymmetric key scenario.

Keywords—Cloud Computing,Authentication,Cryptography,Security

I. INTRODUCTION

Cloud computing is a paradigm for delivery of computing services over the internet, on-demand, as pay as you service. It gives sharing of computing resources without having own servers and storage application. Based on end user requirements, cloud services are categorized into three: Saas, Paas, and Iaas. Software as a Service provides cloud service environment that is accessed through the internet. But the user must have proper license from the cloud service provider. Platform as a Service is one of the cloud services which provides platform for user developing our own application. Infrastructure as a Service is major cloud service environment that provides virtual computing resources like servers, storage devices, operating systems, network on the internet through cloud service providers. Virtual machine reservation services are provided by Cloud computing providers with specified computing units. The main goal of Iaas is reduced the physical maintenance. In cloud computing, data security is arguably the most vital concern and the foremost issue to taken into account. The cloud will presumably hold most sensitive information; hence cloud provider must offer high profiled security. To enhance the security of data deposited to cloud, authentication mechanisms were deployed. One such from cryptography is the technique of writing or storing information in a way that it's revealed only to those to who are intended to receive. In a cloud environment, cryptography is used to prevent data resided in cloud service provider hosts from the malicious attack by using probable encryption technique. It protects sensitive data without delaying information exchange and deliver robust access controls. In cryptography, data security may be ensured by one of two categories of encryption algorithm, namely secret key cryptography and public key cryptography. Only one key used for both encryption and decryption in secret key cryptography, also called symmetric encryption. Two different keys are used for encryption and decryption in public key cryptography, also called asymmetric encryption.

This paper discusses impact of asymmetric encryption mechanisms done by the researchers for data security in cloud. Section 1 shows the overview of cloud computing cryptography techniques and data security in cloud. Section 2, in detail tabularizes the actual research work done on the asymmetric encryption in cloud computing with merits and demerits. Section 3, explains conclusion to the paper done.

II. A SURVEY ON IMPACTS OF ASYMMETRIC ENCRYPTION METHODOLOGY IN CLOUD COMPUTING

S.No	Year	Author	Paper Title	Pros	Cons
1.	2001	Scott Craver Stefan Katzen Beizzer et.al.,	Copyright protection protocols based on asymmetric watermarking.	Embedding process should be robust.	Considerably increases the complexity of watermark verification protocol.
2.	2001	Emmanouil Magkos Panayiotis Kotzanikolaou et.al.,	An Asymmetric Traceability scheme for copyright protection without Trust Assumption.	Easy identification of Traitor.	More time consuming process.
3.	2003	Sung-Cheal Byun and Byung-Ha Aahn et.al.,	Symmetric and Asymmetric Cryptography based Watermarking Scheme for Secure Electronic Commerce via the internet.	Transmitted data include the encrypted digital data and the signature is contained in the same file.	Even if a bit has been changed or wrong key is used, the received data are regarded as violation of features.
4.	2007	Z.Zeghid, M.Machhout, L.Khriji, A.Baganne, R.Tourki et.al.,	A modified AES based algorithm for image encryption.	Much faster than its counterpart.	Hardware resources required to achieve this throughput.
5.	2010	LAI Xvejia Lu Mingxin Qin Lei Han Junsong Fang Wimen et.al.,	Asymmetric Encryption and Signature method with DNA technology.	More powerful and unbreakable cryptographic algorithm Now-a-days.	DNA Cryptography still cannot compete with the electronic computing technology and the Mathematical cryptography.
6.	2010	Lei Zhang,Qianhong wu,Bo Qin,Josep Domingo-Fercer et.al.,	Identity based authenticated asymmetric group key agreement protocol.	Secure against semantically indistinguishable chosen identity and plaintext attacks.	Key secrecy is very low in this protocol.
7.	2011	Tumpa Roy Kamlesh Dutta et.al.,	Mutual Authentication for mobile communication using symmetric and asymmetric key cryptography.	Capability of identifying authority, reduce the computational power.	Computational cost is very high.
8.	2013	Niraj kumar pankaj kupta Monika sahu Dr.Marizvi et.al.,	Boolean Algebra based effective and efficient Asymmetric key cryptography.	Secured data transfer in form of small and large files.	Difficult to decrypt.
9.	2014	Samiksha Shukla Dr.G.Sadashivappa et.al.,	Secure multi-party computation protocol using Asymmetric encryption.	Ensures confidentiality, security and privacy.	In case of one party and one anonymizer the probability of joint malicious conduct is considerable.
10.	2015	Vahid Forutan Robert Fischer et.al.,	Security enhanced network coding through public key cryptography	Protect data transfer in network.	Absence of standard security.
11.	2016	Pu Yue,Li Guodong Zhao Jing et.al.,	Based on the improved RSA keys and compound chaotic system and design of audio encryption algorithm.	Ensure that the encrypted randomness of the audio file.	Large computation, the calculation speed is slow.
12.	2016	Hsin-Te Wu Gwo-Jiun Horng et.al.,	Vehicular cloud network and information security mechanisms.	Non-Repudiation, Authentication and Conditional Anonymity.	Larger amount of packet length in chameleon hashing method creates a lot of loadings.
13.	2017	Shilpa V Mahagonkar Nilma Dongre et.al.,	TEAC: Timed Efficient Asymmetric cryptography for enhancing security in VANET.	Provide security against malicious attacks.	Message to message overhead.
14.	2017	Naveen Kumar Manisa J Nene et.al.,	Chip based asymmetric key generation in hierarchical wireless sensor networks	Fulfill the security requirements of wireless sensor networks like confidentiality, integrity,	Need some additional economical cost for the hardware.

				authenticity and data freshness.	
15.	2017	Sauvik Bal Mrind Kanti Sarkar et.al.,	ACAFP: Asymmetric key based cryptography algorithm using four prime numbers to secure message communication.	Take less memory and less power also.	Computes only small size prime numbers. Difficult to choose large prime numbers then the factorization of the numbers.
16.	2017	Lakshika Singh, Anuj Kumar et.al.,	Secured Information Retrieval from cloud involving OTP and human voice.	Data will be protected by using multi authentications.	High storage is required for this kind of authentication. This kind of authentication can also be extraneously influenced by once sore throat and cold.
17.	2017	Archit Agarwal Satya Jeet Singh et.al.,	Mask ID's based Asymmetric Session key exchange.	Provide confidentiality and authentication. This mechanism helps in preventing any fowl by a system authorized user.	In key pre-distribution, amount of work done in delivering these many keys and if keys are not placed in time then communication will stop.
18.	2018	Bhaskar Marapelli et.al.,	Enhancement of cloud data security by multi cloud data encryption and decryption.	Data uploaded will be more secured.	Security and Governance is more complicated. Creates resiliency issues.
19.	2018	Harshad R.Pawar Dr.Dinesh G.Harkut et.al.,	Classical and Quantum cryptography for image encryption and decryption.	More secure in the case of exchanging multimedia data.	Increase the communication rang and bit transfer rate.
20.	2018	D.N.Wu, Q.Q.Gan X.M.Wang et.al.,	Verifiable public key encryption with keyword search based on homomorphic encryption in multiuser setting.	Less complexity of computation.	Perform better only fewer search keywords.

III. CONCLUSION

Cloud Security using Asymmetric Key Encryption techniques are briefly discussed in this research work. Cloud data needs a high security since it is replicated and shared over the network. This paper gives brief study on various security mechanisms and their pros and cons while used for the protection of data in cloud computing is done for further research.

REFERENCE

[1]. Scott Craver Stefan Katzen Beizzer et.al.," *Copyright protection protocols based on asymmetric watermarking*", IFIP International Federation for Information Processing **2001**.

[2]. Emmanouil Magkos Panayiotis Kotzanikolaou et.al.*," An Asymmetric Traceability scheme for copyright protection without Trust Assumption*", K. Bauknecht, S.K. Madria, and G. Pernul (Eds.): EC-Web 2001, LNCS 2115, pp. 186–195, 2001. Springer-Verlag Berlin Heidelberg **2001**.

[3]. Sung-Cheal Byun and Byung-Ha Aahn et.al.," *Symmetric and Asymmetric Cryptography based Watermarking Scheme for Secure Electronic Commerce via the internet*", W. Chung et al. (Eds.): HSI 2003, LNCS 2713, pp. 607-612, 2003. Springer-Verlag Berlin Heidelberg 2003.

[4]. Z.Zeghid,M.Machhout,L.Khriji,A.Baganne,R.Tourki et.al," *A modified AES based algorithm for image encryption*", World Academy of Science, Engineering and Technology **27 2007**.

[5]. LAI Xvejia, Lu Mingxin,Qin Lei,Han Junsong,Fang Wimen et,al,." *Asymmetric Encryption and Signature method with DNA technology*", Science China Press and Springer-Verlag Berlin Heidelberg **2010**.

[6]. Lei Zhang,Qianhong wu,Bo Qin,Josep Domingo-Fercer et.al.," *Identity based authenticated asymmetric group key agreement protocol*", M.T. Thai and S. Sahni (Eds.): COCOON **2010**, LNCS 6196, **pp. 510–519, 2010**. Springer-Verlag Berlin Heidelberg **2010**.

[7]. Tumpa Roy Kamlesh Dutta et.al.," *Mutual Authentication for mobile communication using symmetric and asymmetric key cryptography*", D.C. Wyld et al. (Eds.): NeCoM/WeST/WiMoN 2011, CCIS 197, **pp. 88–99, 2011**. Springer-Verlag Berlin Heidelberg **2011**.

[8]. Niraj kumar pankaj kupta Monika sahu Dr.Marizvi et.al.," *Boolean Algebra based effective and efficient Asymmetric key cryptography*", 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s) 978-1-4673-5090-7/13/$31.00 ,**2013** IEEE.

[9]. Samiksha Shukla Dr.G.Sadashivappa et.al.," *Secure multi-party computation protocol using Asymmetric encryption*", 978-93-80544-12-0/14/$31.00,**2014** IEEE, 2014 International Conference on Computing for Sustainable Global Development (INDIACom).

[10]. Vahid Forutan Robert Fischer et.al.," *Security enhanced network coding through public key cryptography*", 2015 IEEE Conference on Communications and Network Security (CNS), 978-1-4673-7876-5/15/$31.00 ,**2015** IEEE.

[11]. Pu Yue,Li Guodong Zhao Jing et.al.," *Based on the improved RSA keys and compound chaotic system and design of audio encryption algorithm*", 2016 International Conference on Smart City and

Systems Engineering (ICSCSE) 978-1-5090-5530-2/16 $31.00 ,**2016** IEEE.

[12]. Hsin-Te Wu,Gwo-jiun Homg et.al.," *Vehicular cloud network and information security mechanisms*", 2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE) IEEE-ICAMSE 2016 - Meen, Prior & Lam (Eds).

[13]. Shilpa V Mahagonkar Nilma Dongre et.al.," *TEAC: Timed Efficient Asymmetric cryptography for enhancing security in VANET*", 2017 International Conference on Nascent Technologies in Engineering (ICNTE) **2017** IEEE.

[14]. Naveen Kumar Manisa J Nene et.al.," *Chip based asymmetric key generation in hierarchical wireless sensor networks*", 2017 2nd International Conference for Convergence in Technology (I2CT) **2017** IEEE.

[15]. Sauvik Bal Mrind Kanti Sarkar et.al*.," ACAFP: Asymmetric key based cryptography algorithm using four prime numbers to secure message communication*", 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON) **2017** IEEE.

[16]. Lakshika Singh, Anuj Kumar et.al.," *Secured Information Retrieval from cloud involving OTP and human voice*", 2017 IJSRST VoL.**3** ,Issue.**7** ,Print ISSN: 2395-6011,Online ISSN: 2395-602X, International Journal of Scientific Research in Science and Technology (www.ijsrst.com).

[17]. Archit Agarwal Satya Jeet Singh et.al.," *Mask ID's based Asymmetric Session key exchange*", 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC) **2017** IEEE.

[18]. Bhaskar Marapelli et.al.," *Enhancement of cloud data security by multi cloud data encryption and decryption*", 2018 IJSRST VoL. **4** ,Issue.**5**, Print ISSN: 2395-6011 | Online ISSN: 2395-602X, International Journal of Scientific Research in Science and Technology (www.ijsrst.com).

[19]. Harshad R.Pawar Dr.Dinesh,G.Harkut et.al.," *Classical and Quantum cryptography for image encryption and decryption*", 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), **2018** IEEE.

[20]. D.N.Wu,Q.Q.Gan X.M.Wang et.al.," *Verifiable public key encryption with keyword search based on homomorphic encryption in multiuser setting*", D. N. Wu et al.: Verifiable PEKS Based on Homomorphic Encryption in Multi-User Setting, VoL **6**, **2018**,IEEE Access.

[21]. C. Kaleeswari, P. Maheswari, Dr. K. Kuppusamy, Dr. Mahalakshmi Jeyabalu ,"*A Brief Review on Cloud Security Scenarios* "**2018** IJSRST ,VoL.**4** ,Issue.**5**.

[22]. Sebagenzi Jason, Suchithra. R, "*Scheduling Reservations of Virtual Machines in Cloud Data Center for Energy Optimization",* in International Journal of scientific research in Computer Science and Engineering, Vol **6,** Issue **2**, pp:16-26, December **2018.**

Authors Profile

Ms.M.Ilakiya is a Research scholar in the Department of Computer Science, Alagappa University, Karaikudi, Tamilnadu, India. She has received her M.Sc in Computer Science from Alagappa University, Karaikudi, Tamilnadu in the year of 2018. Her areas of research interest includes Network security, Cloud Computing.

Ms.R.Vijithra is a Research scholar in the Department of Computer Science, Alagappa University, Karaikudi, Tamilnadu, India. She has received her M.Sc in Computer Science from Alagappa University, Karaikudi, Tamilnadu in the year of 2018. Her areas of research interests include Network security, Cloud Computing.

Prof. Dr K.KUPPUSAMY is working as an Professor and Head in the Department of Computational Logistics,Alagappa University, Karaikukdi, Tamilnadu He has received his Ph.D in Computer Science from Alagappa University, Karaikudi, Tamilnadu in the year 2007. He has 27 years of teaching experience at PG level in the field of Computer Science. He has published many papers in International Journals and presented in the National and International conferences. His areas of research interests include Information/Network Security, Algorithms, Neural Networks, Fault Tolerant Computing, Software Engineering, Software Testing and Optimization

Dr J.Mahalakshmi is working as an Taeaching Assistant in the Department of Computer Science, Alagappa University, Karaikukdi, Tamilnadu She has received his Ph.D in Computer Science from Alagappa University, Karaikudi, Tamilnadu in the year 2017. She has 2 years of teaching experience at PG level in the field of Computer Science. She has published many papers in Reputed International Journals and presented in the National and International conferences. Her areas of research interests include Algorithms, Neural Networks, Optimization Techniques, Deep Learning, Cloud Computing.

