International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 04, April – 2017, PP – 01-04

Security Issues & Comparison of Existing Algorithms in Cloud to Support Multicloud

Smitha Krishnan[1], Dr. B. G. Prasanthi[2]
SB College Changanassery,
HoD,,DEPT MCA,,AIMIT,Benguluru

Abstract: Cloud computing is fundamentally altering the expectations for how and when computing, storage and networking resources should be allocated, managed, consume and allow users to utilize services globally. Due to the powerful computing and storage, high availability and security, easy accessibility and adaptability, reliable scalability and interoperability, cost and time effective cloud computing is the top needed for current fast growing business world. Multi cloud is an emerging concept where security is a major issue.

Keywords: Cloud computing, PaaS, IaaS, SaaS, NaaS, BaaS, network service providers for cloud, Encryption and decryption, cloud security.

Literature survey

[1] Manoj Kumar Mohanty proposed Secure Data Storage on the Cloud using Homomorphic Encryption for hybrid cloud framework that addresses the privacy and trust issues and provides encrypted storage with public clouds.[2]Secure Cloud Computing through Homomorphic Encryption by Maha TEBAA, Said EL HAJII analyzes the application of different Homomorphic Encryption cryptosystems[3] Huiguang Chu designed a privacy preserved and security enhanced password manger by using the human unique biometrics attributes in his paper titled Cloud Password Manager Using Privacy-preserved Biometrics[4]Cloud Security Using Third Party Auditing and Encryption Service by Swaroop S. Hulawale Provided a 3rd party security service provider that would not store any data at its end, and its only duty to providing security service.[5]Privacy Protection in Cloud computing by using CryptographicTechnique. Rajapraveen. k. n, Dr. N. K. Prasanna kumara outlines a new fully homomorphic encryption, based on finite automata constructed from one or more boolean function[6]A Cryptographic Scheme for Secure Cloud Computing byAlejandro Llamas and Ra´ul [7]Data Security and Integrity in cloud computing b y Miao Zhou proposed a system with better efficiency in data security using tree based key management.[8]Deep Packet Inspection with Bit-Reduced DFA for Cloud System Haiqiang Wangl, Kuo-Kun Tsengl, and Jeng-Shyang Panl propose a new algorithm about pattern matching for cloud system, First it performs inexact matching to filter out the part of non attack information and then do exact matching to get the final attack information.[9] Double Key Encryption Method (DKEM) Algorithms Using ANN for Data Storing and Retrieval in Cloud Computing .The Implemention and Application of Fully Homomorphic Encryption Scheme byJing-Li Han Ming Yang Cai-Ling Wang Shan-Shan Xu present a new system for searching on encrypted data which combined ABE (Attribute based Encryption) and FHE to enables anyone even without private-key of the encrypted data to search the data.[11] Security Threats in Cloud Computing by Farhan Bashir Shaikh Sajjad Haider will enable researchers and security professionals to know about users and vendors concerns and critical analysis about the different security models and tools proposed.

Introduction:

Today, the most recent paradigm to emerge is that of Cloud computing, which promises reliable services delivered to the end-user through next-generation data centres which are built on virtualized compute and storage technologies Consumer will be able to access desired service from a "Cloud" anytime anywhere in the world on the bases of demand. Computing services need to be highly reliable, scalable, easy accessible and autonomic to support ever-present access, dynamic discovery and computability, consumers indicate the required service level through Quality of Service (QoS) parameters, according to Service Level Agreements (SLAs).

Encryption and Decryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people and decryption is the process of converting encrypted data back into its original form, so that the authorized recipient can understand it.

Encryption schemes are of two types: Symmetric and Asymmetric encryption schemes.

Symmetric Encryption

An encryption system in which the sender and receiver of a message share a single,common key that is used to encrypt and decrypt the message is called as Symmetric Encryption.

Symmetric-key systems are faster, but their main drawback is that two parties wishing to communicate have to exchange the key in a secure way. In addition, scalability is problem as the number of users increase in the network. Due to its secret nature, symmetric-key cryptography is sometimes referred as secret-key cryptography.

Asymmetric Encryption

An encryption scheme is called asymmetric encryption if it uses two keys instead of one key as in symmetric encryption. One key encrypts the data and the other decrypts. It is also changeably referred to as public key cryptography. An important element of the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only its corresponding private key can be used to decrypt them However, the downside is that they are slower than the symmetric schemes due to non-trivial mathematical computations.

That is why this encryption scheme is used only for encryption of small data or keys while symmetric scheme can be used for larger ones.

A large-scale distributed computing paradigm, which provides Data Storage Service, Computing Power and Data Transferring Service, with capabilities of elasticity Software (SaaS), Infrastructure (IaaS), Platform (PaaS), Network (NaaS), Business (BaaS) and Organization as a Service.

Cloud computing can provide three kinds of services, IaaS, PaaS and SaaS. ***SaaS*** means the service provided to client is the applications running on the cloud computing infrastructure. It can access by thin client interfaces such as browser etc.

PaaS refers to deploy the applications created by the development language and tool say Java, python, .net etc. provided by the service providers to the cloud infrastructure.

IaaS refers to the services provided to the users is to lease the processing power, storage, transpiring, network and other basic computing resources, with which users can deploy and run any software including operating systems and applications. To all these services, there is no need for users to manage or control the cloud infrastructure, including network, server, operating system, storage and even the functions of applications. Generally, we have three types Public and Private Hybrid clouds.

When a Cloud is made available in a Pay-As-You-Go manner to the public, we call it a ***Public****Cloud*, The service being sold as Utility Computing. Current examples of Public Utility Computing are Amazon Web Services, Google AppEngine and Microsoft Azure. We use the term ***Private Cloud*** to refer to internal data centres of a business or other organization that are not made available to the public.

Hybrid is the combination of both. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not normally include Private Clouds.

IaaS	**PaaS**	**SaaS**
Amazons Ec2	Google App Engine	Google Appa
Amazons S3	Yahoo Pig	Salesforce's
IBM's Blue cloud		Customer Relation Management System.

•Server is responsible for processes including data replication, key storage, file retrieval, file storage. The security mechanism will be implemented at server side. (NEW)

DIFFERENT ALGORITHM FOR DATA ENCRYPION

Encryption	**Year**	**Inventor**	**Properties**
DES	1971		Symmetric
RSA	1977	Ron Rivest, Adi Shamir and Leonard Adleman,	Asymmetric, Multiplicative
Goldwasser Micali	1984	Shafi Goldwasserand Silvio Micali	Additive, but it can encrypt only a single bit
3DES			Symmetric
EIGamal	1985.	Taher Elgamal	Asymmetric, Multiplicative
BlowFish	1993	Bruce Schneier	Symmetric
Serpent	1998	Ross Anderson, Eli Biham and Lars Knudsen.	Symmetric
Pailleir	1999	Pascal Paillier in 1999	Asymmetric, Additive
Camellia	2000	Mitsubishi and NTT company	Symmetric
Damgard-Jurik Scheme	2001	Damgard & Jurik	Additive
AES	2001	Vincent Rijmen, Joan Daeman	Symmetric
BGN		Boneh, Goh, and Nissim	Many addition but only one Multiplication.
SalSa	2005	Daniel Bernstein	Symmetric
Fully Homomorphic	2009	Gentry	As many multiplication &addition

Conclusion

A best encryption method can be adopted to provide security in multicloud.

References:

[1]. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN (Online): 1694-0814

[2]. Secure Cloud Computing through Homomorphic Encryption Maha TEBAA, Said EL HAJII

[3]. Kuyoro S. O., Ibikunle F. & Awodele O. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 247 Cloud Computing Security Issues and Challenges

[4]. IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 (Nov-Dec. 2012), PP 19-21 Privacy Protection in Cloud computing by using Cryptographic Technique.

[5]. Volume 4, Issue 4, April 2014 ISSN: 2277 128X International Journal of Advanced Comparison among Various Cryptographic Algorithms

[6]. International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 2, Feb 2014. ISSN 2348 – 4853 A Survey on Data Integrity of Cloud Storage in Cloud Computing

[7]. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013 A Survey on Attribute Based Encryption Scheme in Cloud Computing

[8]. *International Journal of Computer Applications (0975 – 8887) Volume 82 – No1, November 2013* An Investigation on the Issues in Cloud Data Security

[9]. Homomorphic Encryption: Theory & Application Jaydip Sen Department of Computer Science, National Institute of Science & Technology Odisha,

[10]. Homomorphic Encryption and the BGN Cryptosystem,David Mandell Freeman

[11]. Comparative study of various Security Algorithms applicable in Multi-Cloud Environment - Ms.Theres Bemila Karan Kundar Lokesh Jain Shashikant Sharma Nayan Makasare

Biography

Ms. Smitha Krishnan is a research scholar in Bharathiar University. Completed MCA from AIMIT Bangalore and currently working as assistant professor in dept of computer science in SB college

Dr. B. G. Prasanthi is the second rank holder in M.Sc., (comp),fifth rank in M.Tech and was district topper in M.Phil and is having her Phd in faculty of Engineering currently working as head for MCA in AIMIT Bangalore. She trained many research scholars, post graduate students of Bangalore and different universities in computer science and technology. She is a reviewer for three IEEE journals and many international and national journals, keynote speaker for many conferences and published 35 research papers in reviewed national and international journals.

