International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Improving Security in Cloud IaaS Services using Cryptography

Dushyant, Dr. Rajeev Yadav
Department of Computer Science and Engineering, Rao Pahlad Singh Group of Institutions, Balana, Mohindergarh, Haryana, India

ABSTRACT

With the internet getting so popular data sharing and security of personal data has gain much more importance than before. Cloud provides and efficient way to outsource the data either online or offline but data security becomes one of the major issues in unreliable cloud environment. In this paper we have provided a brief review on all the different techniques and algorithms used for securing cloud data that is been addressed by existing authors of same domain.

Keywords : IaaS, PaaS, SaaS, Cloud Computing

I. INTRODUCTION

In the most basic cloud-service model & according to the IETF (Internet Engineering Task Force), providers of IaaS offer computers physical or (more often) virtual machines and other resources. To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed.

II. Issues in Cloud IAAS Service

In past few years, cloud computing has grown to one of the fastest growing segments of IT industry. But this growth need cloud security to be intact. Below mentioned are few most important issues of cloud computing.

Privacy

Cloud computing utilizes virtual computing technology. In this, user's personal data is kept on various virtual data centers which may cross international boundaries. This is where data privacy protection may face controversy of various legal systems. There might be few chances that un-legitimate user may leak hidden information, which in turns compromises privacy of data.

Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third

of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

III. Literature Survey

There are many issues with current cloud and their architectures. Some of them are users are often tied with one cloud provider, computing components are tightly coupled, lack of SLA supports, lack of Multi-tenancy supports, Lack of Flexibility for User Interface. [4]

2.1 Cloud Computing Security: From Single to Multi-Clouds

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers. Another example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services. Another example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption.

One of the results that they propose is to utilize a Byzantine flaw tolerant replication convention inside the cloud. Hendricks et al. express that this result can evade information defilement created by a few parts in the cloud. Then again, Cachinet al. assert that utilizing the Byzantine flaw tolerant replication convention inside the cloud is unsatisfactory because of the way that the servers having a place with cloud suppliers utilize the same framework establishments and are physically placed in the same spot. As per Garfinkel, an alternate security hazard that may happen with a cloud supplier, for example, the Amazon cloud administration, is a hacked secret key or information interruption. In the event that somebody gets access to an Amazon account secret key, they will have the capacity to get to the majority of the account's occasions and assets. This paper presents Byzantine flaw tolerant system but it is still vulnerable to dictionary attacks[1].

2.2 Ensuring Data Integrity And Security In Cloud

An alternate approach to secure the information utilizing diverse squeezing and encryption calculations and to conceal its area from the clients that stores and recovers it. The main contrast is that the framework introduced by Olfa Nasraoui is an application based framework like which will run on the customers own framework. This application will permit clients to transfer record of diverse organizations with security peculiarities including Encryption and Compression. The transferred records might be gotten to from anyplace utilizing the application which is given.

The security of the Olfa Nasraoui model has been investigation on the premise of their encryption calculation and the key administration. It has been watched that the encryption calculation have their own particular attributes; one calculation gives security at the expense of fittings, other is solid however utilizes more number of keys, one takes additionally handling time. This area demonstrates the different parameters which assumes a paramount

part while selecting the cryptographic calculation. The Algorithm discovered most guaranteeing is AES Algorithm with 128 bit key size. The main disadvantage of this paper is the key size of AES which can be further extended to 256 bit [2].

2.3 Reliable Re-Encryption In Unreliable Clouds

An alternate methodology to secure distributed computing is for the information holder to store scrambled information in the cloud, and issue decoding keys to approved clients. At that point, when a client is renounced, the information manager will issue re-encryption orders to the cloud to re-scramble the information, to keep the disavowed client from decoding the information, and to produce new unscrambling keys to substantial clients, so they can keep on getting to the information. Then again, since a distributed computing environment is involved numerous cloud servers, such summons may not be gotten and executed by the majority of the cloud servers because of problematic system correspondences. This paper proposes a system which requires periodic key generation and re-encryption techniques which gives overhead of encrypting again and again therefore decreasing the throughput of the system [3].

2.4 Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage

A principle gimmick of cloud is information offering. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng demonstrate to safely, effectively, and adaptably impart information to others in distributed storage. We portray new open key cryptosystems which deliver steady size figure messages such that proficient assignment of unscrambling rights for any set of figure writings are conceivable. The curiosity is that one can total any set of mystery keys and make them as minimized as a solitary key, yet enveloping the force of every last one of keys being accumulated. At the end of the day, the mystery key holder can discharge a consistent size total key for adaptable decisions of figure content set in distributed storage, however the other encoded documents outside the set stay secret. This paper doesn't provide any solution on how data will be stored in cloud. They just use visibility control to hide data from users [5].

2.5 Trusting The Cloud, Security in The Cloud

There are different examination challenges likewise there for embracing distributed computing, for example, generally oversaw administration level assertion (SLA), security, interoperability and dependability. This examination paper diagrams what distributed computing is, the different cloud models and the principle security dangers and issues that are at present inside the distributed computing industry. This exploration paper additionally investigates the key research and difficulties that shows in distributed computing and offers best practices to administration suppliers and also endeavors planning to power cloud administration to enhance their end result in this serious financial atmosphere. This paper addresses many different issues in cloud computing related to administration services [7].

IV. Proposed Methodology

We propose to develop a system that provides data security in Cloud based IaaS services using encryption algorithm and compression algorithms.

Core Objectives

- To develop a website that will provide functionality to upload and download data.
- To encrypt data using AES algorithm (key size: 256).
- To compression data using ultra ZIP.

Data Flow Diagram

Level 0:

Fig 5.1: DFD Level 0

Level 1:

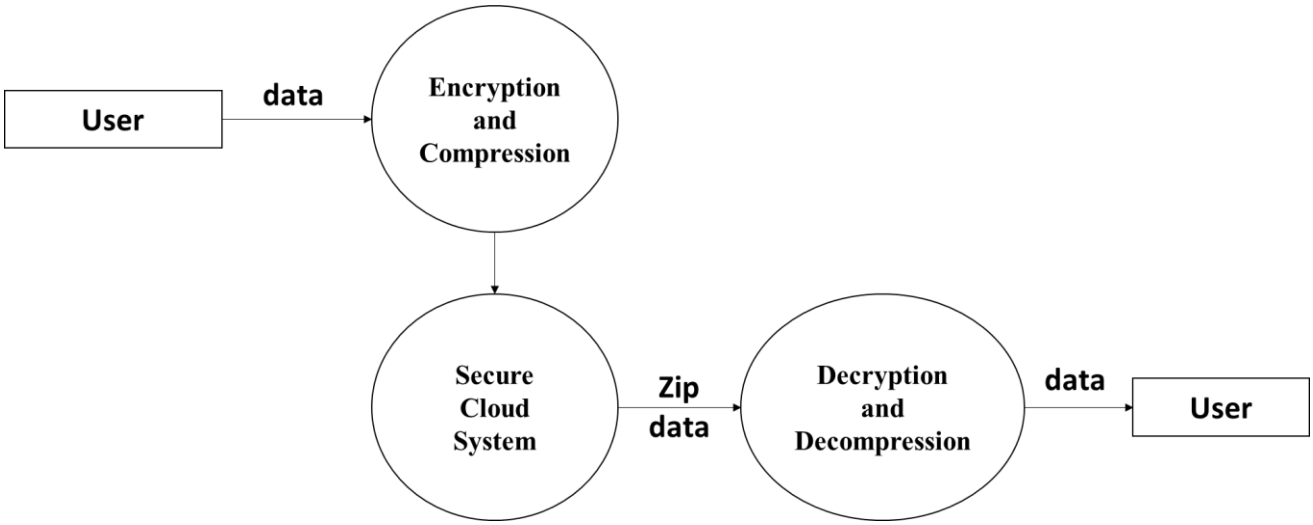


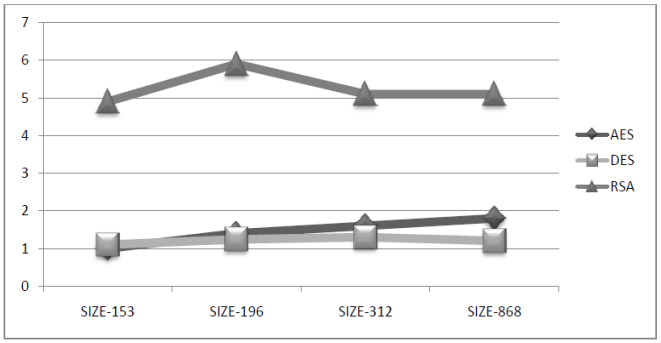
Fig: DFD Level 1

V. RESULTS AND DISCUSSION

Comparison between Symmetric Algorithms

Table Comparison between Symmetric Algorithms

Input	AES	AES Cloud	DES	DES Cloud	BLOWFISH	Desede	Desede Cloud
10 Kb	11.5	1.5	7.5	2	4	12	4.5
13 Kb	14.7	2	10	2.5	4.7	15.5	5.25
39 Kb	21	3	31.5	6.5	8.25	47.25	10.25
56 Kb	24.5	3.75	50.25	9.25	15.7	70.5	14.5



Decryption Time (in milliseconds)

VI. Conclusion

IaaS is the establishment layer of the Cloud Computing conveyance demonstrate that comprises of numerous segments and innovations. Every segment in Cloud framework has its helplessness which may affect the entire Cloud's Computing security. Cloud computing business develops quickly notwithstanding security concerns, so coordinated efforts between Cloud gatherings would aid in

overcoming security difficulties and push secure Cloud Computing administrations. In this paper we have proposed a system that will provide better security in cloud environment. We have proposed a security architecture which provides strong security using AES algorithm.

VII. Future Scope

In future we plan to provide more security to system using multiple encryption algorithm at ones. We also plan to provide file sharing feature in the system so that user will be able to share their file. We will also like to provide an extra feature of data availability which will help increase reliability of system even if one of the server crashes.

VIII. REFERENCES

[1]. Cloud Computing Security: From Single To Multi-Clouds Mohammed A. Alzain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference On System Sciences.

[2]. Ensuring Data Integrity And Security In Cloud Storage Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.

[3]. Reliable Re-Encryption In Unreliable Clouds Qin Liu ,Chiu C.Tan ,Jiewu, And Guojun Wang IEEE Communications Society Subject Matter Experts For Publication In The IEEE Globecom 2011 Proceedings.

[4]. Service-Oriented Cloud Computing Architecture Wei-Tek Tsai, Xin Sun, Janaka Balasooriya 2010 Seventh International Conference On Information Technology

[5]. Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014

[6]. Mell-Peter, Grance-Timothy. September 2011. The NIST Definition Of Cloud Computing.

[7]. C Cachin, I. Keidar And A. Shraer, "Trusting The Cloud", ACM SIGACT News, 40, 2009, Pp. 81-86. Clavister, "Security in The Cloud", Clavister White Paper, 2008.

[8]. HMei, J. Dawei, L. Guoliang And Z. Yuan, "Supporting Database Applications As A Service", ICDE'09:Proc. 25thintl.Conf. On Data Engineering, 2009, Pp. 832-843.

[9]. C Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security In Cloud Computing", ARTCOM'10: Proc. Intl. Conf. On Advances In Recent Technologies In Communication And Computing, 2010, Pp. 1-9.

[10]. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina And Eduardo B Fernandez An Analysis Of Security Issues For Cloud Computing Hashizume Et Al. Journal Of Internet Services And Applications 2013.

[11]. Gehana Booth, Andrew Soknacki, and Anil Somayaji Cloud Security: Attacks and Current Defenses 8th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'13), JUNE 4-5, 2013, ALBANY, NY.

[12]. Brent Lagesse Challenges In Securing The Interface Between The Cloud And Pervasive Systems IEEE Pervasive Computing, Vol. 8, Pp. 14–23, October 2009. [Online].

[13]. Wayne A. Jansen Cloud Hooks: Security And Privacy Issues In Cloud Computing Proceedings Of The 44th Hawaii International Conference On System Sciences – 2011.

[14]. Mukesh Singhal And Santosh Chandrasekhar Collaboration In Multicloud Computing Environments: Framework And Security Issues

Published By The IEEE Computer Society 0018-9162/13/$31.00 © 2013 IEEE

[15]. Sushmita Ruj, Milos Stojmenovic, Amiya Nayak Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.

[16]. Lukas Malina and Jan Hajny Efficient Security Solution for Privacy-Preserving Cloud Services 6TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013

[17]. Morgan, Lorraine Conboy, Kieran FACTORS AFFECTING THE ADOPTION OF CLOUD COMPUTING: AN EXPLORATORY STUDY Proceedings of the 21st European Conference on Information Systems 2012

[18]. Sarita Motghare, P.S.Mohod International Journal of Advanced Research In Computer Science Volume 4, No. 4, March-April 2013

[19]. Bryan Ford Icebergs in the Clouds: The Other Risks Of Cloud Computing SIGCOMM, August 2010

[20]. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.

[21]. Abhinandan P Shirahatti, P S Khanagoudar Preserving Integrity of Data and Public Auditing For Data Storage Security In Cloud Computing IMACST: VOLUME 3 NUMBER 3 JUNE 2012

[22]. Allan A. Friedman and Darrell M. West Privacy and Security in Cloud Computing Number 3 October 2010

[23]. Mohamed Nabeel, Elisa Bertino Privacy Preserving Delegated Access Control in Public Clouds PUBLISHING YEAR 2012

[24]. Myrto Arapinis, Sergiu Bursuc, and Mark Ryan Privacy Supporting Cloud Computing: Confichair, A Case Study University Of Birmingham Nov. 2012

[25]. Darko Androcec Research Challenges For Cloud Computing Economics Nov. 2011

[26]. Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull Security Issues with Possible Solutions In Cloud Computing-A Survey International Journal Of Advanced Research In Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013