Volume 3, Issue 3, March 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Broker Cloud Computing Paradigm Using AES And Selective AES Algorithm

Amanpreet Kaur
Research Scholar, Department of Computer Science
Lovely Professional University, Phagwara
India

Gaurav Raj
Ph.D Scholar, Department of Computer Science
Punjab Technical University
India

Abstract— Cloud computing is highly promising technology because of its unlimited resource provisioning and data storage services which help us in managing the data as per requirements. But this area is still suffering problem of secure storage and communication of data inside the cloud and in between clouds also. Due to the use of internet and vital remote servers to maintain the data and applications, the cloud computing environment becomes open for the attackers to attack on the user data and communication services. This paper mainly focuses on the user authentication and data security over the Broker Cloud Computing Paradigm by exploiting the cryptographic techniques as Selective Encryption using AES. The cryptography technologies offer encryption and decryption of the data and user authentication information to protect it from the unauthorized user or attacker.

Keywords— Cloud Computing, Data Security Issues, AES Technique, Selective Encryption using AES, Broker Cloud Communication Paradigm [BCCP], Cloud Coordinator [CC], Service Level Agreement [SLA].

I. INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing have aimed to allow access to large amounts of computing power in a fully virtualized manner, by aggregating resources and give a picture of a single system. A computing cloud has networks of nodes. Therefore scalability should be a quality feature of the computing cloud. In addition, an important aim of these technologies has been delivering computing as a utility. Cloud computing can be seen as the requirement of three users which are categorized in three modules : -

End user : - just wants to use the application softwares such as Ms Office, Paint Brush, and Image Processing Software etc. This sort of service is provided by Software as a Service model of cloud computing which gives freedom to the user from getting license of software.

Commercial organization : - who wants to spread his business with the help of website then he/she has to set up the servers and maintenance of servers which leads to the high cost. But the cost of infrastructure can be removed by having Infrastructure as a Service model of cloud computing because the storage and security of data maintenance of servers etc is handled by the cloud service provider.

Developer: - It also takes care of the needs of developer by providing the platform on which developer wants to work such as Operating System etc. This is also provided by the Platform as a Service model.

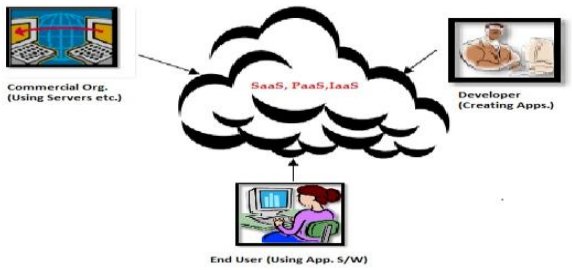


Fig: 1 Cloud Computing

The Cloud Computing technology is embedded with three services which are just one click away, easy to use and pay as you use the service. Software as a Service offers you easy access to various online applications that are being hosted on the infrastructure of a service provider. It frees the end user from getting license for application software etc. Platform as a Service lets the end users in undertaking multiple functionalities like testing, different operating system, queuing management, developing, integrating, managing and securing cloud infrastructure and cloud apps. For instance, Developer can work on that platform which is more suitable for him. Infrastructure as a Service provides excellent configuring and administering infrastructure. For example, it lets the business persons to expand their business without

spending lot of money on servers, software, administration and maintenance of servers etc. The deployment models let the user to implement cloud computing as per the user or organization's requirement. Public cloud is made available to the general public or a large industry group and is owned by an organization selling cloud services. Private cloud is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

II. RELATED WORK

Balachandra Reddy Kandukuri, Ramkrishna Paturi V, DR. Atanu Rakshit[1] states the Service Level Agreement is in the form of document which defines the clear relationship of responsibilities and security policies between the cloud user and vendor along with the security policies. There different security issues that SLA should discuss like privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, long term viability, data availability etc. "Top Threats to Cloud Computing V1.0" [15] paper provides context to assist the organization in making educated risk management decisions regarding the cloud adoption strategies. This papers has tried to focus on some issues are either unique to or greatly increased by the key features of cloud computing i.e it is shared, on demand nature etc to identify the following threats in our initial document such as data leakage, Malicious Insiders, Service Hijacking etc. Traian Andrei[14] illustrates the present state of the cloud computing with its development challenges, academia and industry research efforts are introduced. In spite of this, it also describes cloud computing security problems and represents a model of security architecture for cloud computing implementation. Meiko Jensen, J¨org Schwenk, Nils Gruschka and Luigi Lo Iacon[9] presents a selection of issues of cloud computing security. It is investigated that ongoing issues with application of XML signature and the web services security frameworks, discussed the importance and capabilities of browser security in the cloud computing context i.e SaaS, raised concerns about cloud service integrity and binding issues (PaaS) and sketched the threat of flooding attacks on Cloud Systems (IaaS). Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth[8] have introduced a practical security model based on key security considerations by looking at a number of infrastructure aspects of cloud computing. A well established dynamic security model for the infrastructure of cloud computing solution is essential. The dynamic model offers a horizontal and vertical configurable and policy based security approach. It focuses on the infrastructure scope covered within the domains of network, server, storage and systems management.

The above whole study gives an idea to enhance the security of user authentication information along with user data and the way to secure the data sent between the storage cloud and computing cloud using Selective Encryption using AES Technique.

III. DATA SECURITY ISSUES OF CLOUD COMPUTING

There are number of security of issues which are related to cloud computing which scares the cloud customers to opt it for their business purposes and many more. Each issue is explained and accompanied on potential or real world measured impacts.

(1) **User access rights:** - Cloud customer must have the knowledge about the people who are managing and assuring the integrity of the data because all the services are provided by third party which takes control over the physical, logical and personnel and makes it little bit risky.

(2) **Regulatory compliance:** - To maintain the integrity of the data is the responsibility of the customer even when it is kept by the service provider. Regulatory compliance aims that corporations or public agencies to ensure that personnel are aware of and take steps to meet the terms of relevant laws and regulations.

(3) **Data location constraints:** - When use the cloud, user is not known to the location where the user data is hosted. User must ask providers that can they store and process data in specific jurisdictions and whether they can make an agreement to follow privacy requirements.

(4) **Assurance of better encryption techniques:** - The cloud provider should confirm that encryption schemes are designed and tested by experienced testers. It should be assured that encryption accidents will not make data unusable or more encryption will not affect data availability.

(5) **Recovery of data from disasters:** - Even if cloud user has no control over the data and not aware of data location then a cloud provider should give clear answer about availability and complete recovery of data in case of disaster. How much time they will take to recover the data?

(6) **Law enforcement:** - It is very difficult to investigate illegal activities in cloud computing because logging and data for multiple users is co-located and data may also be spread across an ever-changing set of data centres.

(7) **Data availability:** - Ideally, your cloud computing provider will never go broke or overtaken by a larger company. But if this happen then your data that it will remain available even after such an event.

IV. PROBLEM DEFINITION

Cloud Computing is not secure computing model because there are many data security issues. The data security is provided to the data which is stored in storage cloud by using the encryption technique. But still there is a loophole through which the data integrity can be compromised i.e when data is moving from the storage cloud to computational cloud for processing. So, in this thesis we are going to secure data in this stage to make the cloud computing more reliable technology for customers.In the below diagram, first of all data owner asks for the task execution from the broker. After this, broker again asks data owner for the task specification and data owner submit its task specification.

Thereafter broker sends task specification to the cloud exchange to get the available clouds. Cloud exchange sends request to all connected cloud coordinator to provide their current status with available resources needed to complete the execution of the task. Cloud coordinator updates the available data center of the cloud to cloud exchange. Cloud exchange gives information of available of all clouds and data centres to broker. Broker asks data owner to send encrypted data using AES cryptography technique. Finally broker receives encrypted data from data owner and forwards this data to the cloud exchange to storage cloud to store the data and whenever data will move from the storage cloud to computational cloud. Then again it will be encrypted at storage cloud and sends to the cloud exchange to transfer it to to the available computational cloud for the execution of the task.

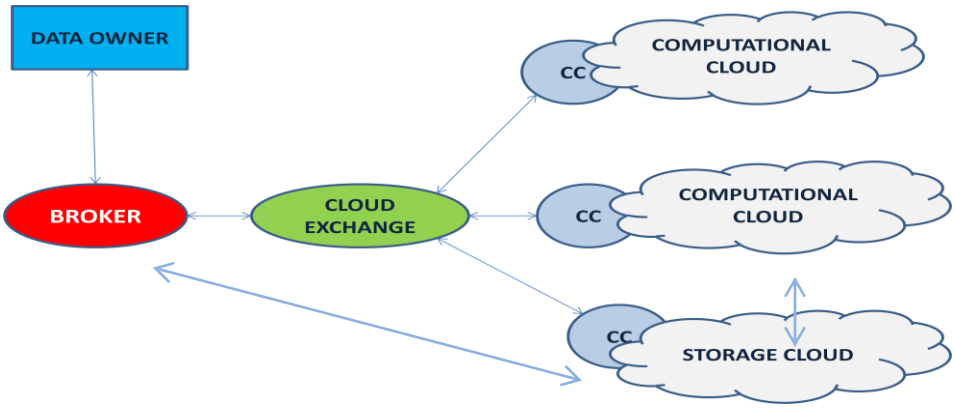


Fig: 2 Purposed Security Approach

Legends:
CC :- Cloud Coordinator

V. Purposed Work

Broker Cloud Communication Paradigm for Data Security: -

Data security is major issue when it is about to transfer the data through wired or wireless network. Nowadays it is very difficult to take data physically from one place to another place because it is very time consuming. On the contrary, with the help of internet it is very easy to transfer the data. To secure data over the internet, we come across with large number of Encryption/Decryption Techniques which converts the plain text into the cipher text. These Encryption/Decryption Techniques convert the readable content in non readable content and only authenticated sender and receiver can get the original readable content therefore it is helpful in enhancing the data segregation issue using Selective Encryption using AES Technique.

1. User logins with username and password. Thereafter send it in encrypted form (Using Advanced Encryption Standard to the Broker.
2. Broker will decrypt login information using Advanced Encryption Standard and also check the SLA of the client as per his/her login information. Finally user is allowed to access the account.
3. User asks for Service.
4. Broker asks for task specification.
5. User Submits task specification
6. Broker requests for available storage cloud to Cloud Exchange as per the client's SLA Service
7. Cloud Exchange asks clouds for their current status of available resources
8. Clouds send their current status info to Cloud Exchange
9. Cloud Exchange sends list of available clouds as per SLA's requirement to Broker
10. Broker tells user to send data

Legends:
CC :- Cloud Coordinator

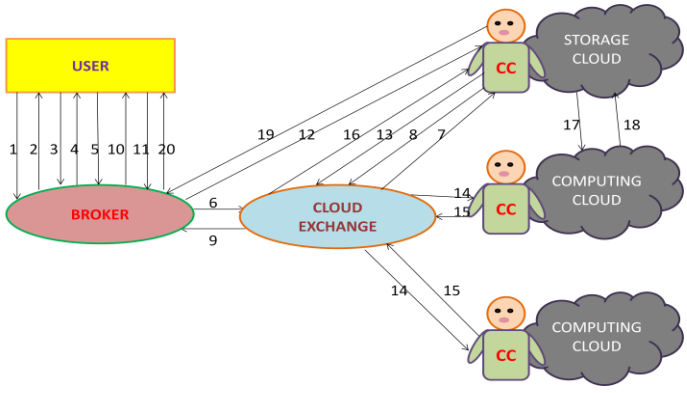


Fig. 3 Enhanced data security approach over Storage Cloud and Computing Cloud

11. User sends encrypted data (Selective Encryption using AES Algorithm) to broker
12. Broker sends encrypted data to Cloud Coordinator to store it on virtualized Storage Server.
13. Storage cloud asks Cloud exchange for available computational cloud for data processing.
14. Cloud Exchange asks computational cloud for their status with available resources
15. Computational Clouds send their current status to Cloud Exchange.
16. Then cloud exchange sends current status to storage cloud
17. Storage cloud sends encrypted data (Selective Encryption using AES Algorithm) to the Computing cloud for processing
18. Computational clouds decrypt encrypted data (Selective Encryption using AES Algorithm), process it and send back to storage cloud in encrypted form
19. Storage cloud sends encrypted data (Selective Encryption using AES Algorithm) to the broker.
20. Broker sends encrypted data to data owner.

VI. IMPLEMENTATION ANALYSIS

Implementation phase will contain two security algorithms i.e Advanced Encryption Standard and Selective Encryption using AES for the data security. These two security algorithms will be applied on different modules of my purposed secured approach for data. Cloud Analyst simulator will help in analyzing the performance of both security algorithms in different modules. In CloudAnalyst, we are going to incorporate five classes for this purposed secure approach named as user, broker, cloud exchange, storage cloud and computing cloud. In this approach, we are considering three modules to secure the data transmission among all these modules. Proposed paradigm can classified as

a. Security over User and Broker Communication: - This module provides the security over user's login information which is going to be exchanged between the user and broker by using Advanced Encryption Standard.

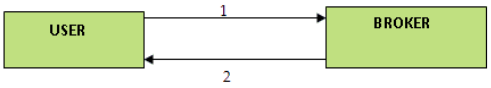
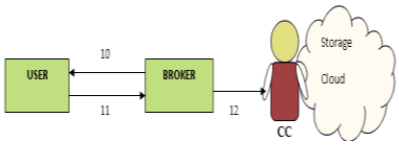


Fig: 4 Secure User-Broker Communication

The above diagram describes that the user can access all the services by getting login into its account as authenticated user. Broker will decrypt login information using Advanced Encryption Standard and also check the SLA of the client as per his/her login information. Finally user is allowed to access the account.

b. Security over Broker and Storage Cloud Communication: - It depicts the communication procedure to store the cipher text onto storage cloud. It also lets the broker to access the data from storage cloud. Mainly the data movement from the broker to storage cloud and storage cloud to broker is protected by the use of Selective Encryption using AES Technique. Cloud Coordinator works as inter-mediator between cloud and its users. It also supports the load balancing and data center provisioning according to service requirement. The communication between broker and cloud coordinator to store the data is depicted as follows: -

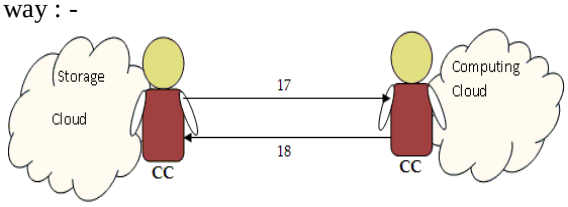


:

Fig: 5 Secure Broker-Storage Cloud Communication

Broker tells the user to send data User sends encrypted data (Selective Encryption using AES Algorithm) to broker. Broker sends encrypted data to Cloud Coordinator to store it on virtualized Storage Server.

c. Secure communication between storage cloud and computing cloud: - In this, whenever the data needs any type of processing then data moves from the storage cloud to computing cloud. This is the major source for the attackers to hack the user contents therefore the data is sheltered with Selective Encryption using AES Technique. The communication takes place in this way : -



#

Fig: 6 Secure Storage Cloud-Computing Cloud Communication

Cloud Coordinator of Storage cloud sends encrypted data (Selective Encryption using AES Algorithm) to the Computing cloud for processing Cloud Coordinator of Computing cloud receives the encrypted data and then allocate it to data center for its decryption of encrypted data (Selective Encryption using AES Algorithm), process it and send back to

storage cloud in encrypted form.

VII. CONCLUSION AND FUTURE WORK

In this paper, we purposed an enhanced secured approach for data transmission with Advanced Encryption Standard Technique and Selective encryption using AES Technique. We mainly focus on enhancing the data security in cloud computing while transferring data from the data owner to broker, broker to storage cloud and vice versa and storage cloud to computational cloud and vice versa. I will test the Performance and throughput of these two security algorithms through CloudAnalyst Simulator. There is also need to embed the security relevant files by extending the structure of CloudAnalyst toolkit for more protected environment. In the future, researchers can try to reduce the routing overheads to provide higher throughput. Besides this, the communication between broker and cloud exchange can be encrypted to protect it from different types of Denial-Of-Service Attack.

REFERENCES

[1] Balachandra Reddy Kandukuri, Ramkrishna Paturi V, DR. Atanu Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing

[2] "Cloud computing Benefits, risks, recommendations for information security cloud computing" November 2009, http://www.enisa.europa.eu

[3] Huiming Yu, Nakia Powell, Dexter Stembridge and Xiaohong Yuan, "Cloud Computing and Security Challenges", 2012 ACM Publication

[4] Kamal Dahbur, Bassil Mohammad and Ahmad Bisher Tarakji, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing"

[5] La'Quata Sumter, "Cloud Computing: Security Risk", 2010 ACM Publication

[6] Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms to Enhance The data Security of Cloud in Cloud Computing", 2012 VSRD International Journal of Computer Science & Information Technology

[7] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", 2010 International Journal of Computer Applications

[8] Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth, "A Layered Security Approach for Cloud Computing infrastructure", 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009 IEEE.

[9] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing

[10] Mark Townsend, "Managing a Security Program in a Cloud Computing Environment", 2009 ACM Publication 978- 1- 60558-661-8/09/09

[11] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security", 2012 VSRD International Journal of Computer Science & Information Technology

[12] Narjeet Singh and Gaurav Raj, "Security on BCCP through AES Encryption Technique" 2012 International Journal of Engineering Science & Advanced Technology

[13] Sherif El-etriby, Eman M. Mohamed, Hatem S. Abdul-kader," Modern Encryption Techniques for Cloud Computing, Randomness and Performance Testing", 2012 ICCIT Journal

[14] Traian Andrei, "Cloud Computing Challenges and related Security Issues", 2009 A survey Paper http://www.cse.wustl.edu/~jain/cse571- 09/ftp/cloud/index.html

[15] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0" http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010

