IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Enhanced Security as a Service to Protect Data in Public Cloud Storage

S. Balamurugan[1], Dr. S. Sathyanarayana[2]

Research Scholar, Dept. of Computer Science, Bharathiar University, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Dept. of Computer Science, Sreekanta 1st Grade College, Mysore, India[2]

Abstract: Cloud provides computing resources as an on-demand service. The main service of cloud is data storage. It has different datacentre to maintain and monitor user data. It is more reliable storage but it has many security related issues. To address this security issues in the cloud, this paper proposes a security framework comprises of three main services for security, key and storage. Security is provided as a service to users. This framework consists of two security services for different types of data. Users have to choose any one security service based on their choice. Key generation is another service in the framework which provides key for security service by the way of sending the key directly to the users. Keys used for security service are not known to other cloud service in the framework. The framework protects attacks from inside and outside the cloud. It enhances the security in the public cloud environment.

Keywords: Cloud Storage; Security Service; SECaaS; KaaS; STRaaS;

I. INTRODUCTION

Cloud computing is a modern computing paradigm which enable users to get cloud services in anywhere at any places[1]. Cloud has three basic service models that are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), four deployment models that are Private, Public, Community and Hybrid clouds and five essential characteristics that are on-demand service, broad network access, resource pooling, rapid elasticity and measured service[2].

The essential characteristics promote a lot of benefits in cloud computing environment and also cloud is differed from other computing by these characteristics. One of the familiar services from cloud is its storage [3]. Users with computer devices can access any services from the cloud. It provides huge amount of virtual storage to keep the users' data. Users outsource their data to cloud. But they don't have control on their data in the cloud. Data in the cloud are controlled and monitored by the cloud service providers.

Beyond the advantage of cloud, it has so many issues and challenges like security, scalability, resource allocation and etc. Among these issues security is the top most concern in the cloud environment. Data is stolen by insiders as well as outsiders. Insiders are attackers from the authorized personnel from cloud provider's side. Outsiders are attackers from outside the cloud such as other users of cloud services[4]. To protect this type of security breaches, it is necessary to have a security framework.

This paper proposes a security framework to address the security problems in cloud environment. This framework comprises of two main services for security, key and storage. Users can use the security services to secure their data in cloud. Cloud storage is vast space which is used to store the users' data.

II. RELATED WORKS

Monikandan S et al. [5] have proposed to enhance security framework for cloud storage. The framework has three cloud services which are used to improve the security of data stored in the cloud storage, namely, SEaaS, KGMaaS and STaaS. SEaaS has three different security service algorithms, namely, AROcrypt, MONcrypt and AROMONcrypt. These algorithms are used to hide the users' data before they are uploaded to the cloud storage. Users should select any one of the security service algorithms to secure their data in the cloud. Each algorithm is used to hide a particular type of data. The users need not hide all the data uploaded to the cloud; instead, they can encrypt or obfuscate only necessary data. SEaaS is provisioned to the users to encrypt or obfuscate the sensitive data only, which may be numerical or non-numerical or both. Users should choose any one of the algorithm based on the type of particular data. Keys are directly forwarded to the users. The users' details are received from SEaaS to KGMaaS.

Victor Chang et al. [6] has developed a framework called Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. Authors are demonstrated that CCAF multi-layered security can protect data in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and

DOI 10.17148/IJARCCE.2016.54105

3) convergent encryption. To validate CCAF, it has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 trojans and viruses. The CCAF multi-layered security can block 9,919 viruses and trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated.

Kamara et al., [7] proposed a cloud data storage framework for public cloud. The framework consisted of four components, namely, a Data Processor (DP), that processes data before they are sent to the cloud; a Data Verifier (DV), that checks whether the data in the cloud have been tampered with; a Token Generator (TG), that generates tokens which would enable the cloud storage provider to retrieve segments of customer data; and a Credential Generator (CG) that implements an access control policy by issuing credentials to the various users. This framework is designed in the scenario for both general and enterprise users. In the case of general users' scenario, they install the components of the framework that consists of a DP, a DV and a TG into their local machine. In the case of enterprise users' scenario, Medium-sized enterprises deploy dedicated machines within their network including a DP, a DV, a TG and a DG. If enterprises are very large, the prospect of running and maintaining dedicated machines to process all employees' data are infeasible. More precisely, in this case the dedicated machines only run data verifiers, token generators and credential generators while the data processing is distributed to each employee. In this framework, users have to maintain the components like DP, DV, TG and CG. Cloud is used only for storing the data. Users have the maximum responsibilities to execute this framework.

Yau et al., [8] presented an approach to secure the users' data from service providers. The approach contained three main parts, 1) separating software service providers, and infrastructure service providers, 2) hiding data owners' information in cloud and 3) data obfuscation. The approach consisted of seven entities namely, Software Cloud, Infrastructure Cloud, Software Service Broker, Infrastructure Service Broker, Software Service Attestation Authority, Data Obfuscator and Data De-obfuscator. The Software Cloud and Infrastructure Cloud have the same features of the software layer in ordinary cloud computing architecture. However, the software layer and infrastructure layer are not managed by the same service provider. The Software Service Brokers and Infrastructure Service Brokers have the same functionality of the service brokers in Service Oriented Architecture (SOA), but they have the additional function for identity anonymization. The Software Service Attestation Authority, Data Obfuscator and Data De-obfuscator are additional entities in this approach.

Atiq ur Rehman et al., [9] proposed a framework to preserve confidentiality of data stored in Cloud Database as a Service (DaaS) model. The proposed framework stores sensitive data with a combination of encryption and obfuscation techniques. The framework consists of four modules namely, Encryption, Obfuscation, Metadata and Query optimizer. Encryption and obfuscation are used to encrypt and obfuscate the data respectively. Encryption and obfuscation are done before sending the data to the cloud DaaS. Metadata is maintained by cloud users for storing details of keys and for encryption and obfuscation techniques. Query optimizer is used to enable users' query to run on the encrypted and obfuscated data in the cloud storage. The four modules in the framework are executed from the users' side. Cloud users have more responsibility to generate the key and also to keep the key secured.

Basescu et al., [10] proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. They have designed the framework to detect and stop a large number of attacks defined through an expressive policy description language and to be easily interfaced with various data management systems. They have showed that they could efficiently protect a data storage system by evaluating their security framework on top of the BlobSeer data management platform [Nic, 09]. The benefits of preventing a DoS attack targeted towards BlobSeer were evaluated through experiments performed on the Grid5000 test bed [Jeg, 06].

Govinda et al., [11] proposed an agent-based security framework for ensuring security. It helps users to control their sensitive information, and also ensures that the users have fewer burdens at their side. It assists the users by communicating their security related preferences to the service providers and assists the service providers in compliance with security law and regulations. An essential feature of agent-based security is obfuscation, used by users to protect the security of the data. Agent should control two entities namely; Obfuscator that obfuscates the data sent by user to the cloud, Data Retriever that retrieves the data sent by cloud to users. Agent could automatically obfuscate some or all the fields in a data structure before they are sent off to the cloud for processing, and translates the output from the cloud back into de-obfuscated form. The obfuscation and data retrieval are done using a key which is chosen by the agent and not revealed to CSP. Simple obfuscation technique can easily be broken. There is a need for proper SLA among users, agent and cloud providers.

Munir et al., [12] proposed a cloud security framework that identifies security challenges in cloud computing. The framework contains the following components. 1) *Client*: Users could access the client side with Multi-Factors Authentication (MFA) provided by End-User Service Portal (EUSP). 2) *End-User Service Portal*: When clearance is granted, a Single Sign-on Access Token (SSAT) could be issued using certification of user. Then the access control component shares the user information related with security policy and verification with other components in EUSP and CSPs. 3) *Single Sign-on (SSO)*: It enables user to access multiple applications and services

DOI 10.17148/IJARCCE.2016.54105

in the cloud computing environment through a single login. 4) *Service Configuration:* The service enabler makes provision for personalized cloud service using user's profile. 5) *Service Gateway and Service Broker:* A service gateway manages network resources and VPN on the information lifecycle of service broker. 6) *Security Control*: It provides significant protection for access control, security policy and key management against security threats. 7) *Security Management*: It provides the security specification and enforcement functionality. 8) *Trust Management*: It is a challenging need of integrating requirements driven trust negotiation techniques with fine-grained access control mechanisms. 9) *Service Monitoring*: An automated service monitoring system guarantees a high level of service performance and availability.

Hamdan Al-Sabri et al., [13] proposed Cloud Storage Encryption (CSE) architecture by using encryption techniques to provide a high level of data protection to cloud storage. The CSE architecture allows to encrypt and to index data in a manner that ensures the protection of data.

The proposed architecture is composed of seven components. 1) *Director generated Keys and privileges*: A center within the organization to generate public and private keys for data users, as well as granting special privileges to the suitable roles inside the organization. 2) *Data users*: Clients or employees within the organization. 3) *User Roles*: It determines the characteristics and privileges for users. 4) *Encryption Point*: It is used to encode and index the data and divide data into several packages. Each package is stored in different cloud servers. A specific code is included in the divided packets, so that it can be assembled during the retrieval. 5) *Searchable Encryption*: It is a technique to search for the encrypted data during the retrieval of data from cloud storage without decryption. 6) *Decryption Point*: It is used to decode the encrypted data retrieved from cloud storage. 7) *Cloud Data Storage*: Databases for data storage. Users should maintain this architecture with all components. It increases the user encumbrance.

Manpreet K et al., [14] presented a Cipher Cloud framework. It helps users to keep their data confidential on public cloud. The framework uses a two-step encryption process, by which all the data sent from the users to cloud and cloud to users are retained completely encrypted. A thorough security control is needed to protect the most sensitive data that may not be guaranteed in the public cloud computing architectures.

III.PROBLEM DEFINITIONS

Data protection is top most security issue in cloud. Users' data in the cloud are attacked by hackers from outside Cloud Service Providers (CSP) called outsider attack and inside the CSP called insider attack. Attacks from inside the CSPs are very difficult to be protected or to be identified.

Users' data sent to the cloud are controlled and monitored by CSPs. CSPs as privileged administrators have the rights to look into the users' data. So, there is a possibility that insiders from CSPs attack the data. Users do not have any control of the data in cloud storage. Moreover, cloud is a public environment. Data may mingle with other users' data.

Users do not know whether the data are encrypted in the cloud storage or not. Maintaining keys for each user is more difficult for CSPs, and the same key is used for all users' data. Users' data have to be in a fixed format specified by the service provider, and hence the service provider knows all the information required for understanding users' data. Here the data protection issues are raised up.

IV.METHODOLOGY

The proposed framework uses three cloud services to improve the security of data stored in the cloud storage, namely, SECurity as a Service (SECaaS), Key as a Service (KaaS) and STorage as a Service (STRaaS). Three different CSPs provide these services. SECaaS provides two security service algorithms, namely, ESSAE [15], ESSAO. Figure 1 represents the methodological diagram of proposed framework.

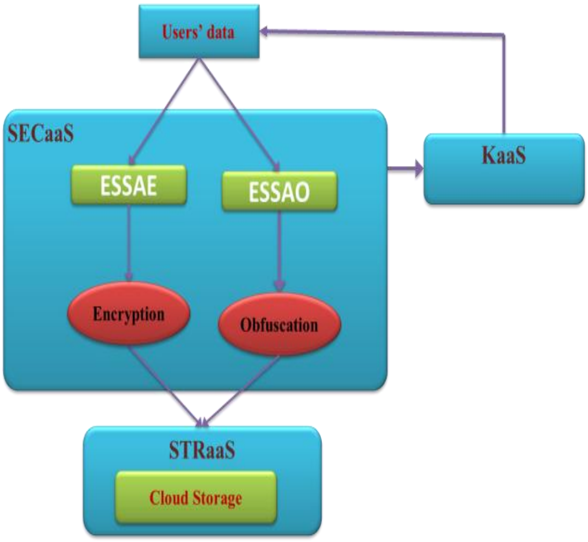

Figure 1. Methodology Diagram of Proposed Framework

Users can choose any one security service based on their data type. ESSAE is used to process the non-numerical data. ESSAO is used to process the numerical data. Non-numerical data are encrypted by ESSAE and Numerical data re obfuscated by ESSAO.

V. PROPOSED FRAMEWORK

The proposed framework is depicted in the figure 2. It has three services namely SECurity as a Service (SECaaS), Key as a Service (KaaS) and StoRage as a Service (STRaaS). SECaaS provides two security service algorithms namely ESSAE and ESSAO.

DOI 10.17148/IJARCCE.2016.54105

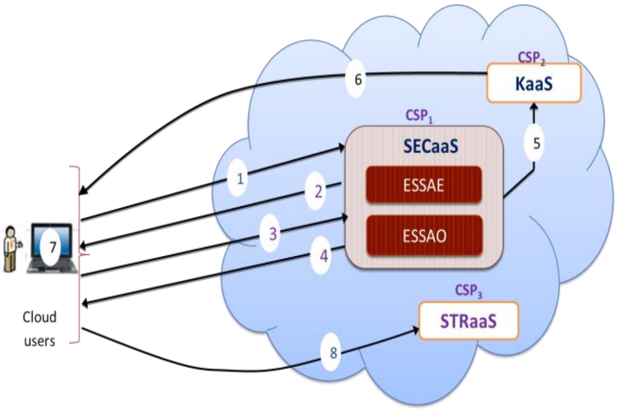

Figure 2. Proposed framework

Step involved in the proposed framework is as follows:-

1. *User request for data upload.*
2. *SECaaS provides details of security services available.*
3. *User chooses a security service and type of the data based on their requirement*
4. *SECaaS sends an executable file for the security algorithm.*
5. *SECaaS in CSP_1 instructs the KaaS in CSP_2 to provide keys to the users who would choose particular algorithm in SECaaS. SECaaS sends the details of selected ESSA and users related information to KaaS.*
6. *KaaS generates keys suitable for the ESSA by the users. Keys are directly communicated to the users and not through CSP_1.*
7. *Users submit the data along with keys to the ESSA to encrypt or obfuscate the data.*
8. *Once the data are encrypted or obfuscated, they are uploaded to the cloud storage of CSP_3.*

A. SECaaS

SECaaS is one of the cloud services in the framework. It provides two security service algorithms. ESSAE is mainly used for non-numerical data. ESSAO is mainly used for numerical data. ESSAO can also reduce the size of the data being uploaded ESSAE is based on symmetric encryption. ESSAO is based on symmetric obfuscation SECaaS provisions users to protect their data from insiders as well as outsiders.

B. KaaS

KaaS generates the keys for the SSAs in SECaaS. Generates the key using a key generation algorithm such as random number generation and forwards the keys to the users directly. KaaS sends an acknowledgment regarding the status report of key generation to SECaaS. KaaS maintains a log for the key generation and management.

C. STRaaS

Cloud storage is maintained, managed and backed up remotely and made available to users over the internet. Online backup is a strategy for backing up users' data that involves sending a copy of the data over a proprietary or public network to an off-site cloud storage server. Backup procedure improves the reliability of the data in cloud storage.

VI. EXECUTION OF PROPOSED WORK

SECaaS provide security services from the cloud to the users. The users should choose a security service in SECaaS, based on the selected SSA the users' data are encrypted or obfuscated or both. Consider the Educational Institutions (EI); If EI wants to store data shown in Table I into the cloud storage, they should decide which type of data is to be converted from readable into unreadable. If EI wants to hide the numerical type data of Students' like Roll No, Marks, Total and Average, then they should choose the ESSAO security service.

TABLE I: SAMPLE STUDENTS' MARKS DETAILS

R. No	**Name**	**Class**	**Sub1**	**Sub2**	**Sub3**	**Sub4**	**Sub5**	**Tot**	**Avg**
14001	S.Malar	MCA	77	51	60	91	80	359	71.8
14002	P.Venkat	MCA	52	72	70	82	58	334	66.8
14003	W.Venis	MCA	96	53	73	62	92	376	75.2
14004	S.Ananthi	MCA	89	83	90	74	63	399	79.8
14005	M.Lavanya	MCA	84	54	97	69	75	379	75.8

The result of the ESSAO security service is shown in Table II. The result shows that only numerical type data fields are obfuscated.

TABLE II OBFUSCATED DATA USING ESSAO

R. No	**Name**	**Class**	**Sub 1**	**Sub2**	**Sub3**	**Sub 4**	**Sub5**	**Tot**	**Avg**
A	S.Malar	MCA	)	)	0	Y	Space	Q	@
F	P.Venkat	MCA	2	@	$	D	$	F	+
)	W.Venis	MCA	Space	{	S	$	0	@	{
2	S.Ananthi	MCA	S	K	&	D	#	C	Space
(	M.Lavanya	MCA	2	D	C	;	{	9	2

If EI wants to hide the non-numerical type data of Students' like Name, Class then they should choose the ESSAE security service.

The result of the ESSAE is shown in Table III. The result shows that only non-numerical type data fields are encrypted.

TABLE III ENCRYPTED DATA USING ESSAE

R. No	**Name**	**Class**	**Sub 1**	**Sub 2**	**Sub 3**	**Sub 4**	**Sub 5**	**Tot**	**Avg**	**Res**	**Grd**
14001	hdP(<EK$5	BB1.2.	77	51	60	91	80	359	71.8	).7.Ru	/xZunlVN
14002	4Iu084k.G	.R.^UU	52	72	70	82	58	334	66.8	M1'./.	#zS"#1p=~
14003	I\yzft!2/	V…||	96	53	73	62	92	376	75.2	Dgu.k.	SK:WV8RiJ

DOI 10.17148/IJARCCE.2016.54105

14004	%Bf8eJ4lr	?.G.qq	89	83	90	74	63	399	79.8	j.~.^.	15vEc)F>S
14005	)>[jphgp]	}}’.C.	84	54	97	69	75	379	75.8	L.’$3.	^]?hpQiA

VII. ADVANTAGES OF PROPOSED FRAMEWORK

1. Framework helps the users to protect their data from internal as well as external threads.
2. It helps user to protect their sensitive data only.
3. It contains different services for security, key and storage
4. Security service provides a encryption algorithm to protect the data from unauthorized access
5. Key service provides key for encryption and its is stored in the user side and not communicated to the CSP.
6. Storage service provides space for store the user data in encrypted manner.

VIII. CONCLUSION

Cloud provides reliable storage of data through maintaining backup copies of data in different cloud data centres. Attackers hack users’ data in the cloud from any data center. The attackers either privileged users from CSP or other users of cloud storage. Attacks by the CSPs are very tough to protect. The proposed framework is developed to secure the data in cloud storage. The framework consists of three different services, namely, SECaaS, KaaS and STRaaS. All these three services have different procedures each. Framework secures the cloud storage environment from different attacks. Simulation study is conducted for the framework in the cloud environment. Simulation results show that the proposed framework achieves its aim by having separate cloud service providers for security, key generation and storage.

REFERENCES

[1] S. Srinivasan, “Cloud Computing Basics, Springer Briefs in Electrical and Computer Engineering”, *Springer Science, Business Media*, pp.61-80, 2014.

[2] Mell P and Grance T., “The NIST Definition of Cloud Computing”, *Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States*, 2011.

[3] Subashini S and Kavitha V., “A Survey on Security Issues in Service Delivery Models of Cloud Computing” *Elsevier Journal of Network and Computer Applications*, Volume 34, No 1, pp. 1-11, 2011.

[4] Dr. L. Arockiam, S. Monikandan. Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering. 2013; 2(8), 3064-3070.

[5] Dr. L. Arockiam, S. Monikandan, “AROMO Security Framework to Enhance Security of Data in Public Cloud”, International Journal of Applied Engineering Research, Print ISSN 0973-4562, Online ISSN 1087-1090, Volume 10, Number 9, (Special Issue), 2015, pp. 6740-6746.

[6] Victor Chang and Muthu Ramachandran, “Towards achieving Data Security with the Cloud Computing Adoption Framework”, IEEE Transactions on Services Computing, pp.1-14, 2015.

[7] Kamara S. andLauter K., “Cryptographic cloud storage”, IFCA/ LNCS 6054, Springer-verlag, Berlin Heidelberg, 2010, pp.136-149.

[8] Yau SS, An HG. “Confidentiality protection in cloud computing systems”, International Journal Software Informatics, Volume 4, Issue 4, 2010, pp. 351-365.

[9] Atiq, U.R. and M. Hussain, “Efficient cloud data confidentiality for DaaS”, International Journal of Advanced Science and Technology, volume 35, 2011, pp.1-10.

[10] Basescu C., A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, “Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies”, *Proceedings of IEEE International Conference on Advanced Information Networking and Applications*, 2011, pp. 459-466.

[11] Govinda K. and Sathiyamoorthy E. “Agent Based Security for Cloud Computing using Obfuscation”, Elsevier Journal, Science Direct, Procedia Engineering, 2012, pp. 125-129.

[13] Hamdan M. Al-Sabri and Saleh M. Al-Saleem, “Building A Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security”, *International Journal of Computer Science Issues*, Volume 10, Issue 2, 2013, pp. 259-266.

[14] Manpreet Kaur and Rajbir Singh, “Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing”, *International Journal of Computer Applications*, Volume 70, Issue 18, 2013, pp.16-21.

[15] S. Balamurugan, Dr. Sanjay Pande, “Symmetric Cryptosystem to Enhance Data Security in Public Cloud Storage “,International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 16, 2015, pp. 37515-37522.

BIOGRAPHIES

S.Balamurugan is working as Head & Asst. Professor in Meenaakshi Ramasamy Arts and Science college – Thathanur, Ariyalur (Dt), Tamilnadu, India. He has 10 years of experience in teaching and 4 years of experience in research. He is completed his M.Sc., and M.Phil. in Bharathidasan University, Tiruchirapalli in 2003 and 2005 respectively and also doing his part time Ph.D degree in Bharathiar University, Coimbatore. He has attended International and National Conferences, Seminars and Workshops. He has published 5 research articles in journals. His research interest is Network Security, Cloud Security and Web Technology.

Dr. S. Sathyanarayana ADSE [Honours] is working as Asst. Professor in Srekantha first grade College, Mysore, Karnataka, India. He has 15 years of experience in teaching and 5 years of experience in research. He is completed his M.Sc., in Karnataka Open University and also completed Ph.D degree in EIUSA University. He has attended International and National Conferences, Seminars and Workshops. He has published 5 research articles in journals. His research interest is Decision Supporting System (DSS) and Information Technology.

DOI 10.17148/IJARCCE.2016.54105