Secured Cloud Data Storage—Prototype Trust Model for Public Cloud Storage

D. Boopathy and M. Sundaresan

Abstract Cloud computing is a business word in information technology world. Cloud-based applications and its related businesses are rapidly growing in the day-to-day world. The small and medium enterprises' concerns are rapidly adopting cloud-based business service models because they are concerned only about the operational cost (OP-EX) and the capital expenditure (CAP-EX) is not essential. The cloud computing has undergone many issues like scalability, reliability, compliance cross-border data storage, multi-tenant, data security, downstream, and regulatory issues. The major issue under high controversy is data storage in cloud. Data confidentiality, data integrity, data authentication, regulation, and legal jurisdictions are the major pests that infect user's business. Taking all these in mind, this paper discusses and proposes a model for data security in cloud storage and its safety measures.

Keywords Secured cloud storage · Cloud issues · Data storage · Cloud security · Data security · Cloud data security

1 Introduction

Cloud computing is rapidly replacing the business era with its wide range of service models. The CSPs' are widely spreading their service with their own and shared business models [1, 2]. The own and shared business models are basically designed and extracted from some open-source models. But the core things of cloud computing have never changed. There are different types of business models available

D. Boopathy (✉) · M. Sundaresan
Department of Information Technology, Bharathiar University,
Coimbatore, Tamilnadu, India
e-mail: ndboopathy@gmail.com

M. Sundaresan
e-mail: bu.sundaresan@gmail.com

S.C. Satapathy et al. (eds.), *Proceedings of International Conference on ICT for Sustainable Development*, Advances in Intelligent Systems and Computing 408, DOI 10.1007/978-981-10-0129-1_35

so the users are confused to choose the better cloud service providers for their purpose [3]. Naturally the user's data will be stored outside the user's premises so the users easily lose their control over the data, which are stored in online cloud storage [4]. If the users lose their control over their data, automatically they are locked with their cloud service provider.

The word trust will rule the cloud computing era [5, 6]. Unfortunately there are no proper standardized international laws and regulations to protect the user's data [7]. The national laws and regulations are framed by some countries and followed by them strictly as a national security. But this is not sufficient to control the data which are stored across their own country border limit [8, 9]. Many countries are protecting their own user's data with basic laws and regulations in the name of belief. This is not sufficient to protect the data which are stored, processed, and transferred in public cloud storage [10].

2 Cloud Computing and Cloud Models

The users are allowed to log into a network-based service, when the vendor provides and operates all the user-required applications from simple to complex levels in the remote machines owned by themselves or by third party companies. The characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Cloud computing is divided into two types. They are cloud service models and cloud deployment models (Fig. 1).

The cloud service model contains three types, they are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [2, 3]. The cloud deployment model contains four types, they are private cloud, public cloud, community cloud, and hybrid cloud [2, 3].

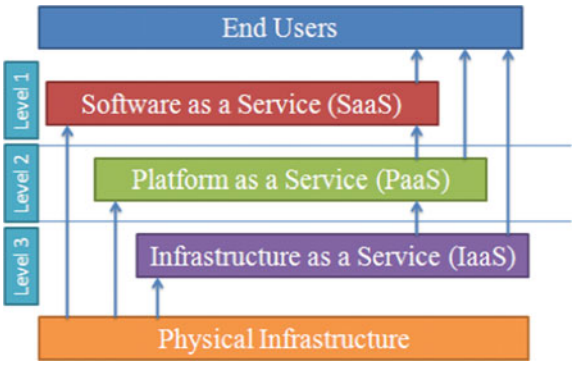

Fig. 1 Cloud service models

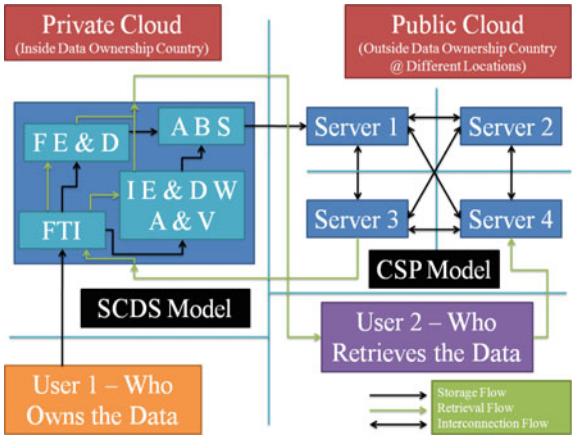

Fig. 2 Secured cloud data storage—prototype trust model

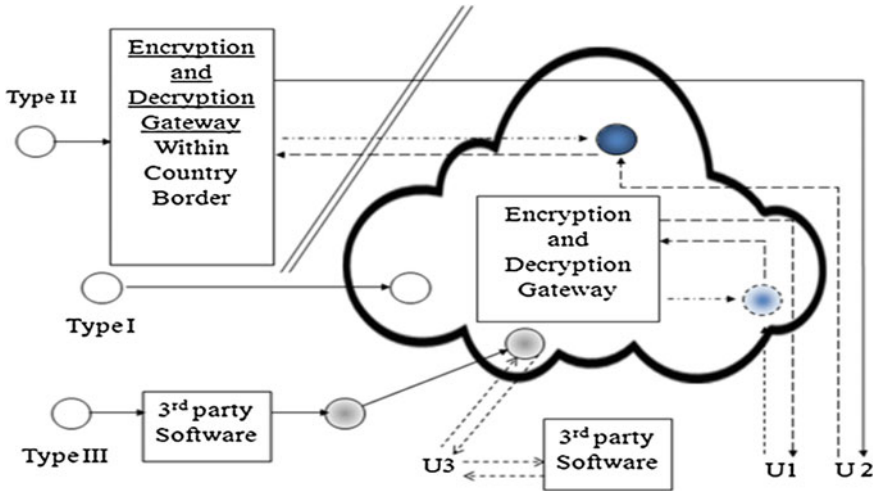

Fig. 3 File encryption and decryption process in SCDS

3 Problem Statement

The cloud computing issues are vast. In this paper, the problems are classified under three different types. The three types are social/user issues, service provider issues, and jurisdiction, regulation, and governance issues.

Social/User issues contain problems such as data protection and security, zero trust mechanism, data confidentiality, data integrity and availability, vendor locked in, and so on. Service provider issues include problem like vulnerabilities of client

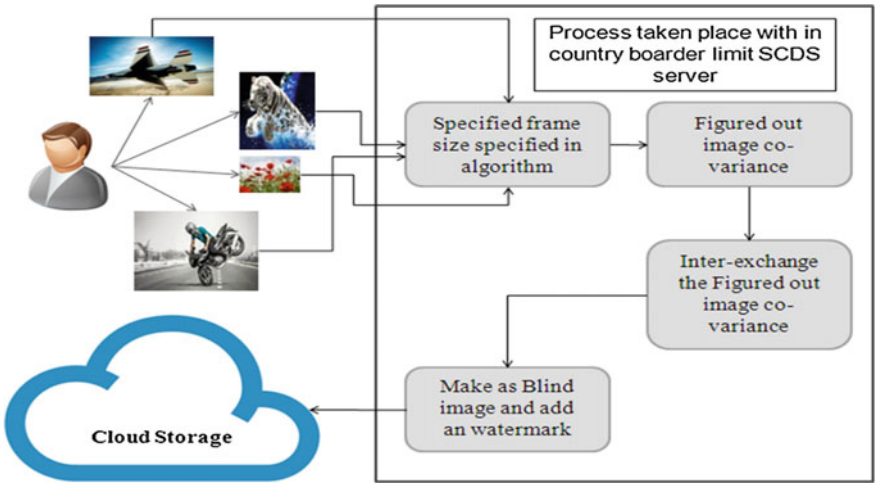

Fig. 4 Image encryption and decryption process using covariance in SCDS

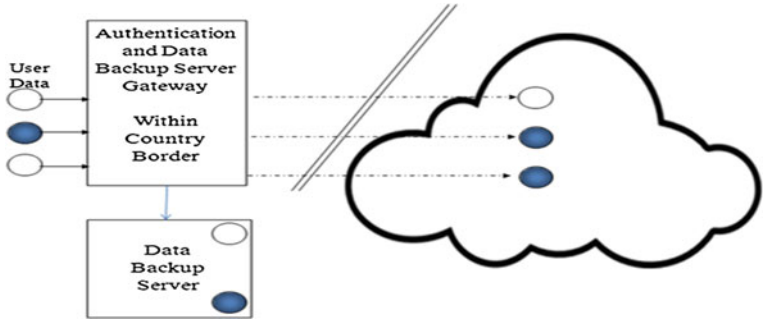

Fig. 5 Automatic data backup model process in SCDS

software, third party vendor issues, multi-tenant model issues, and non-transparency SLA. The jurisdiction, regulation and governance issues includes problem like different jurisdiction limits, no proper standardization and centralized regulations, SLA is eligible to file a suit?—SLA related problems.

4 Objective

The cloud providers are not storing any information within the data owner's country border limit. If the data are not residing within the country limit, then automatically the control on data problem and other data security related problem arises. To overcome the cloud data related issues; creating a new encryption

standard and preparing a new regulation for providing cloud service will put a dot for data related issues in cloud storage. Keeping these things in mind, this model was prepared and proposed with four modules to provide the source to destination level security for the data which will store in cloud storage.

5 Secured Cloud Data Storage

When the users' data are ready for transfer to the cloud storage, before that storage of the data needs to cross the checkpoint within their country border limit. The check point process is called Secured Cloud Data Storage process herein after as SCDS. The SCDS contains four modules they are Data Type Identification Module herein after as DTI, Encryption and Decryption Gateway Server Module herein after as E&DGS, Digital Watermark Allocation and Verification Server Module herein after as DWA&VS, and Automatic Data Backup Server Module herein after as ADBS.

The SCDS is a method of pipeline process. It denotes that the modules are designed independently and then merged together to create this SCDS model. So, if this model needs any update or modification, it will take place only at the specified module only. Here pipeline process stands for coupling each module with other modules for the reason of continuous process (Fig. 2).

5.1 File Type Identification (FTI) Model

Once the data enter into the SCDS, first it moves that data into FTI module. The FTI module is a process of verifying the file data type using its file extension. This process is used for identifying the data type for the reason to figure out the data whether it is sensitive one or nonsensitive one. This FTI process will declare all the types of image file as sensitive data and will declare nonimage file as nonsensitive data.

This FTI process will filter the file in sensitive and nonsensitive manners. After the data type identification, the sensitive data will be transferred to the DWA&VS module and the nonsensitive data will be transferred to the E&DGS module.

5.2 Encryption and Decryption Gateway Server (E&DGS) Model

In E&DGS, data will be encrypted using the public key crypto system. The users will encrypt the file using their public key and then the person who needs to access

the information, that person needs to use the private key to decrypt the file. The existing public key crypto algorithms are not suggested for use for this E&DGS module. The existing algorithms are revealed algorithms and known by public to all. So, the public key crypto algorithm going to be implemented in E&DGS module, need to be a newly developed algorithm or an enhanced algorithm from the existing algorithm.

The reason for this condition is simple; Snowden reveals that RSA security group weakens in their random number generation algorithms on encryption software, and hardware due to order of their local government and security agencies. And also some of the software and social web network portals fix backdoors with in it to collect and surveillance the user information without their knowledge. If we are going with existing and revealed algorithms, we cannot able to trust the security for the data stored in cloud storage. In that cases cloud security will became myth. So, going with existing algorithm, this E&DGS module cannot give assurance for the cloud trust model (CTM) (Fig. 3).

5.3 Digital Watermark Allocation and Verification Server (DWA&VS) Model

If the data are declared as sensitive data, then the data file is any one of the image format types only. There are 25 different types of image formats available.

Before entering into the Digital Watermark Allocation (DWA) process something needs to be generalized. Because the image may have different frame size and vary from file capacity size. So, each and every image needs to be fixed into specific format frame using the lossless method. Using this method any frame size of image will be fixed into the frame, then the image covariance needs to be calculated. Once the covariance is figured out, it will be inter-exchanged using the public key crypto system, and later that image will be changed into blind image that is after inter-exchanging the covariance, that covariance inter-exchanged image will turn into one specific color. It is helpful at the time of loss of data or leakage of information. The inter-exchanged covariance code will be removed only by the prepared programing method.

The DWA process will be reversed at the time of accessing the information. Once the image is accessed with the prior and authorized user, the watermark will be removed first and then the blind image will processed into inter-exchanged covariance method. Then the inter-exchanged covariance will be processed into normal covariance method to get and give the image to the users. Before the data are sent to the user, this module may reframe that image into original image frame size or it may transfer that image in the fixed frame size too (Fig. 4).

5.4 Automatic Data Backup Model

The DTI identifies the data type and forwards the sensitive data into DWA&VS and nonsensitive data into E&DGS. After the DWA&VS process on sensitive data or E&DGS process on nonsensitive data, the processed data will store one backup copy on Automatic Data Backup Server (ADBS), which is located within the country's border limit. After that processed data will transfer to the cloud service provider's storage and replicated in the cloud service providers multiple servers to avoid some issues like service downtime and service crashes from any one server (Fig. 5).

6 Results and Discussion

The secured cloud data storage (SCDS) model was designed in Network Simulator 2 (NS2) to check whether the model is possible or not.

Figure 6 is the NS2 SCDS designed model and its data flow results between the user storage, storage in multiple servers, data request from user to access the data from cloud are shown in Table 1. These mentioned conditions are simulated in NS2 then outputs and results are showed that this SCDS model is possible to implement in an effective manner.

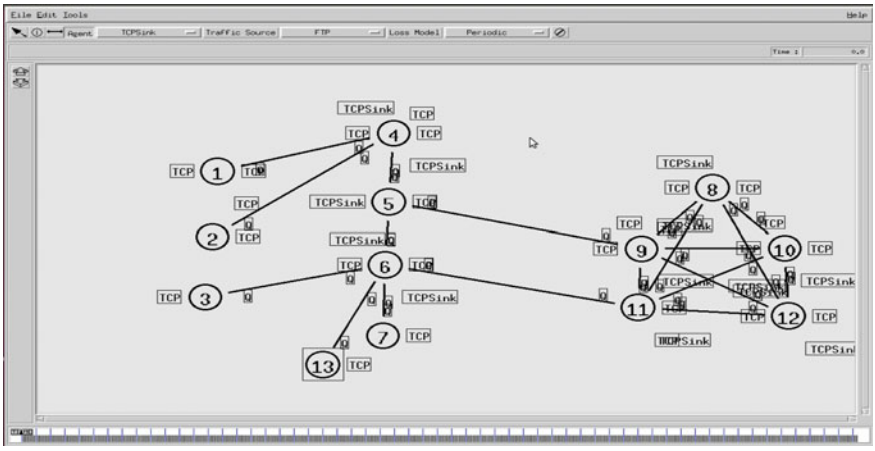

Fig. 6 SCDS—prototype trust model simulated in NS2

Table 1 Process time taken by secured cloud data storage prototype trust model

Time taken to reach each process	Time (ms)	
Data from user to FTI server	100	100
DTI identification time	1.5	1.5
File encryption time	2564	–
Image encryption time	–	2985
ABS time	100	100
Time taken to reach the cloud servers	250	250
Total time taken by SCDS to process a file	3015.5	3436.5

7 Conclusions and Future Scope

Data confidentiality is assured using the Encryption and Decryption Gateway Server (E&DGS) and Digital Watermark Allocation and Verification Server (DWA&VS). The data availability and vendor locked in issues will come to an end using the Automatic Data Backup Server (ADBS). The Data Type Identification (DIT) will avoid the mismatched file formats' uploads, it will avoid the data became vulnerable due to the storage user. The encryption algorithm is in need of enhancement or new level of algorithm development and then the newly developed algorithm will be used only for this SCDS model. If the algorithm is kept as secret, it is not that much easy to reveal and break the algorithm's encryption and decryption systems (like bullrun, hillclimp). The back door fixing, data surveillance on stored data by other country, and illegal use of user data is not possible. The only one issue that may raise is SCDS processed data will be stored on many cloud storages and that data are replicated and mirrored in multiple servers to avoid the downtime issue and server crash issue. But any one of the servers may be attacked by hackers and they may take out the information and data from that server. The encrypted information needs decryption to know exactly what it contains. If the stolen data need decryption it must reach the E&DGS or DWA&VS to finish the reversing process. Once the server is hacked and data information are leaked out, the server information will reach the SCDS processing center automatically. And the data of hacked server will be kept on alert mode. Once the stolen data reach the E&DGS or DWA&VS, it will not allow that data to decrypt.

The DTI, E&DGS, DWA&VS, and ADBS are individual and autonomous processes that are coupled together to provide the SCDS model. So, if the data are stolen from the server due to any issue, and it will not be able to use by the person who stole that. Because the encryption and decryption processes always take place only on SCDS model with in the data owner's country border limit.

Issues like lack of governance on data, different countries jurisdiction issues, and its related issues cannot be solved within rapid manner and also it is not possible in short time. So, preventing the data in effective manner will avoid these types of issues and also avoid the data became vulnerable on cloud storage. Once this level is achieved, this SCDS model will be treated as trust cloud model for data storage in public cloud storage.

References

1. Yu, X., & Wen, Q. (2010). A view about cloud data security from data life cycle. *International Conference on Computational Intelligence and Software Engineering (CiSE)*, 10–12 December 2010 (pp. 1–4).
2. Boopathy, D., & Sundaresan, M. (2014). Data encryption framework model with watermark security for data storage in public cloud model. *International Conference on Computing for Sustainable Global Development*, 5th–7th Mar, 2014 (pp. 903–907).
3. Boopathy, D., & Sundaresan, M. (2013). Location based data encryption using policy and trusted environment model for mobile cloud computing. *Second International Conference on Advances in Cloud Computing*, 19th–20th September 2013 (pp. .82–85).
4. Youssef, A. E., & Alageel, M. (2012). A framework for secure cloud computing. *IJCSI International Journal of Computer Science Issues, 9*(4), 487–500.
5. Sivashakthi, T., & Prabakaran, N. (2013). A survey on storage techniques in cloud computing. *International Journal of Emerging Technology and Advanced Engineering, 3*(12), 125–128.
6. Bhuvaneswari, J., & Vaishnavi, R. (2013). Data security and storage in cloud computing. *International Journal of Emerging Technology and Advanced Engineering, 3*(1), 100–101.
7. Tripathi, A., & Yadav, P. (2012) Enhancing security of cloud computing using elliptic curve cryptography. *International Journal of Computer Applications* (0975–8887)*, 57*(1), 26–30.
8. Huaglory, T. (2012). Security issues in cloud computing. *IEEE International Conference on Systems, Man, and Cybernetics*, October 14–17, 2012, COEX, Seoul, Korea (pp. 1082–1089).
9. Shaikh, R., & Sasikumar, M. (2012). Trust framework for calculating security strength of a cloud service. *International Conference on Communication, Information & Computing Technology (ICCICT)*, Oct. 19–20, 2012, Mumbai, India, pp. 1–6.
10. Ahmad, S., Ahmad, B., Muhammad Saqib, S., & Muhammad Khattak, R. (2012). Trust model: Cloud's provider and cloud's user. *International Journal of Advanced Science and Technology, 44*, 69–80.