A Review Paper for Storage and Computation on Enterprise Data in the Cloud

Khushboo R. Shrote
Department of CSE, Government College of Engineering, Amravati, India,

Pushpanjali Chouragade
Department of CSE, Government College of Engineering, Amravati, India

ABSTRACT
Cloud computing provides way to share information. This Information is secured at cloud ends only. Any third party intruder may hack confidential information. While outsourcing its business-critical data and computations to the cloud, an enterprise loses control over them. How should the organization decide what security measures to apply to protect its data and computations that have different security requirements from a Cloud Service Provider (CSP) with an unknown level of corruption? The answer relies on the organization's perception about the CSP's trustworthiness and the security requirements of its data. This paper proposes a decentralized, dynamic and evolving policy-based security framework that helps an organization to derive such perceptions from knowledgeable and trusted employee roles and based on that, choose the most relevant security policy specifying the security measures necessary for outsourcing data and computations to the cloud.

Keywords: Service provider, CSP, Credentials, Encryption, Decryption

1. INTRODUCTION
In IT enterprises, different computing needs are provided as a service. The service providers take care of the customers' needs, for example, maintaining software or purchasing expensive hardware. In addition, there are many benefits of using the technology available from cloud service providers, such as access to large-scale, on-demand, flexible computing infrastructures. However, increasing the dependability of cloud computing is important in order for its potential to be realized. An organization possesses various types of data that have a wide range of sensitivity. Parts of these data such as customer data, engineering designs etc. are business-critical for which confidentiality, integrity and availability could be very important for the survival or growth of the organization. Employees need to access data of different sensitivity according to their roles in the organization. The users of enterprise data are not restricted to employees of the organization in question, it could be any other individuals like ordinary customers, or employees belonging to other organizations as clients, suppliers or partners. With the advent of cloud computing, an organization often faces the question of whether to outsource all these data and computations to what is known as a public cloud. It has several technological, organizational and environmental factors to consider. Cloud computing research shows that security is one of the most important technological factors that inhibit cloud adoption. It includes concerns about loss of control over data, dissolution of the concept of perimeter security, trustworthiness of CSPs. data confidentiality, integrity, data and service availability, software vulnerabilities, legal and trans-border issues about data location and data privacy etc. When data and computations are outsourced to the cloud, the organization confers a certain degree of trust on the CSP to take proper security measures to protect its data and applications from external as well as from insider attacks. Although the organization can sign security SLAs with the CSPs, monitoring whether these are being properly implemented is yet another task the organization has to perform. Sometimes, it is not even clear who should perform this monitoring activity, the CSP, the organization or a trusted third party. Therefore, organizations must build their own perception about how the CSP will behave i.e. to what extent it can be trusted with different items of data and computations. This will help building policies to retain control over data and computations outsourced to the cloud.

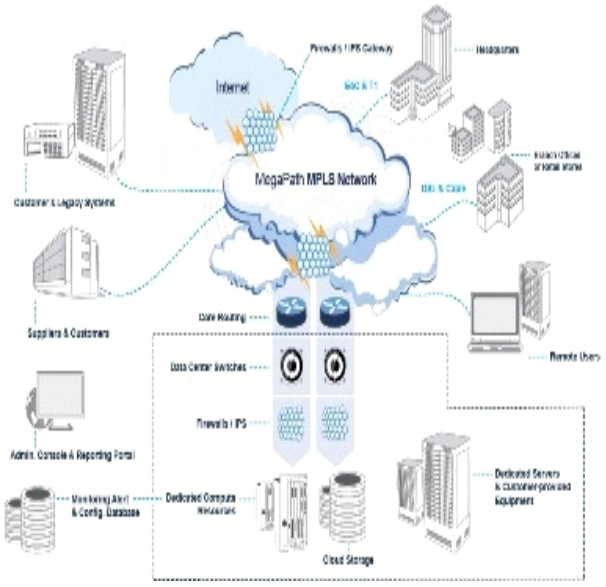

Figure 1. Enterprise Cloud

2. RELATED WORK
2.1. Secure Storage and Computation in Cloud
Several recent works in cloud computing focus on storage and computation security. proposes a system architecture allowing organization-wide integration of untrusted public storage cloud. The architecture guarantees confidentiality, availability and integrity while requiring only a minimum level of trust on the cloud. It uses Information Dispersal Algorithms (IDA) to ensure availability, and by combining symmetric encryption with IDA, achieves high confidentiality. Integrity is ensured by using AES-CMAC operation mode for encryption which

produces a MAC for each data fragment and enables replacement in case of any integrity violation. presents a similar, advanced architecture where the end-devices inside an organization are considered to be within a Personal Secure Cloud or π-Cloud controlled by the π-Box that acts as an intermediary between the π-Cloud and the external cloud. π-Box performs all security operations for data storage and distribution such as information dispersal, encryption, checksum etc. Data is first dispersed using an IDA, encrypted and signed and then the shares are distributed to multiple clouds. When the user inside the organization needs to access data, the shares are fetched from the multiple clouds and the data is reconstructed if enough shares could be withdrawn. proposes a cryptographic cloud storage service consisting of the following components:

1) A data processor that processes data before being sent to the cloud;
2) A data verifier that verifies whether data stored in the cloud has been tampered with;
3) A token generator that generates token to enable the CSP to retrieve customer data segments
4) A credential generator that implements access control policy by issuing credentials to various parties in the system.

It allows integrity, confidentiality as well as secure data erasure. The authors suggest the use of searchable encryption to enable confidentiality and retrieval of data based on keywords and attribute-based encryption to enable implementation of credentials and proof of storage to verify integrity. suggests a general-purpose protocol for securely computing any function in the cloud without revealing any information about the input or output by using multiple VMs. The usage of principles of secure multi-party computation (SMC) ensures that if at least a single VM is honest, no information is revealed. In our work, we also use similar methods, derived from the literature of secure multi-party computation. has proposed the Twin Cloud architecture for securely outsourcing data and arbitrary computations to the cloud. It consists of the usage of two types of clouds, the trusted cloud (such as a private cloud) which performs all security-critical operations such as encryption, decryption etc. and the untrusted commodity cloud which performs all performance-critical operations on encrypted data.

2.2. ASCII-BCD Based Steganography

Steganography can be of two types :

1) Fragile: This steganography involves embedding information into a file which is destroyed if the file is modified.
2) Robust: Robust marking involves embedding information into a file which can not be easily destroyed.

The customer needs to store confidential information in the cloud for effective access. The customer information is applied into ASCII-BCD based encryption algorithm which used to generate the encrypted information. This algorithm is deployed in the deployment. The encrypted data are handled by the cloud controller who controls the entire cloud. The entire cloud controller controls all worker nodes and handles the virtual model(CDM). The CDM has various features to enable effectiveness over the cloud machines properly. The cloud can store customer's data with various security measures which are not known by the cloud customer. A multilevel security is applied over the cloud in order to protect the data during the travel between the two end i.e. customer end to cloud end and vice versa. The overall process of the proposed ASCII-BCD algorithm is based on image steganography techniques. Two phases occur ASCII-BCD based conversion phase and Steganography phase.

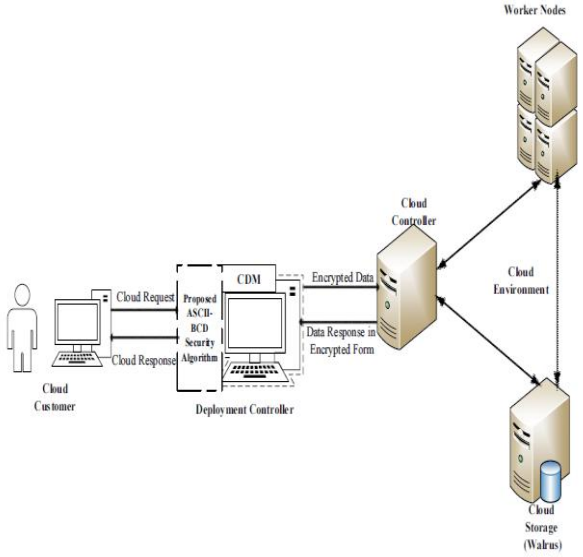

Figure 2. Architecture of the proposed Algorithm

2.3. Conceptual Diagram

Figure 3 describes that the conceptual diagram of the proposed algorithm. An input section reads the data from input source file then it is converted into ASCII-BCD based data by using security keys. The conversion section generates all the cipher text and then this partial cipher text are converted into a complete cipher text using another key. A complete cipher text is send to the cloud for storage using encryption section. If a customer need the data from the cloud, first it reads an image, identifies the position in the image and then it converts the image into BCD form. The partial cipher text is then converted to an equivalent ASCII character by using the decryption key. The original text is recovered by using another key with decryption process.

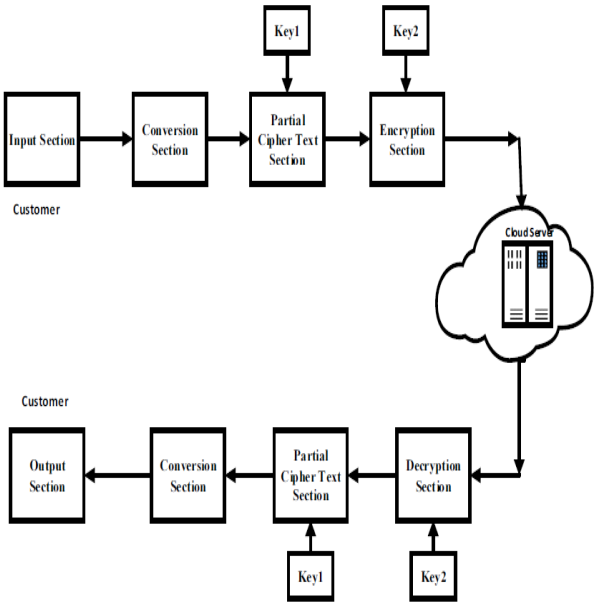

Figure 3. Conceptual diagram of Proposed algorithm

2.4 ALGORITHMS

Encryption Algorithm

ASCII_Based_SteganoEncryption ()

Begin i=0;

TextFile ← Input_Read (); //Reading the Text file for

each(character ← TextFile) do// Reading the character

begin

IM [] ←character;

IC←IM[i];

AIC←ASCII (IC); // ASCII conversion of input character

BIC←BCD (AIC); // BCD conversion of AIC

PIC←Position[IC];// Position of the input character

APIC←ASCII (PIC); // ASCII value of PIC BPIC←BCD

(APIC); // BCD value of APIC

Partial_Cipher [] ← (BIC) XOR (BPIC);// generation of

partial cipher text Key1← Key_Gen (); // key generation

Full_Cipher [] ← (Key1) XOR (Partial_Key []);// generation

of full cipher text

BFC [] ← BCD (Full_Cipher []);//BCD conversion of full

cipher text IImage←Image_Read ();

PIImage [] ← Pixel_Position (IImage); for each position ←

PIC do Image_Position ← Set_Pixel (BFC []); //set the pixel

over the image

end;

i++;

end; *FirstCiphetText←Key2 [Full_Cipher[0]];// pointer to

the first cipher text

End: Encrption_Process ()

Decryption Algorithm

ASCII_Based_SteganoDecryption ()

Begin i=0;

ImageFile ← Image_Read ();//Reading the image file for each

pixel ← ImageFile do

// Reading the pixel position

begin

IM [] ←pixel;

BIP←IM[i];

Key2← Key_Gen (); // key generation

BPartial_Cipher [] ← (Key2) XOR (BIP);

// generation of BCD partial cipher text BIMPP←

get_Image_Pixel_Position ();

// reading the image pixel position;

OBC []←(Key1)XOR(BPartial_Cipher []); // BCD based

output character

AOBC [] ←ASCII (OBC [])// ASCII conversion of BCD

based output character

OC [] ← character(AOBC []);// character conversion of

AOBC

end;

for each character ← OC [] do TextFile← character;

end;

End: Decryption_Process ()

3. CONCLUSION

In this paper we have proposed a policy-based review paper which is highly evolving and dynamic for securely outsourcing enterprise data and computations. This framework, unlike other related works in the literature, elaborately takes into account varying user perceptions, gathered in a decentralized way directly from the users, about trustworthiness of CSPs and data security requirements to formulate secure data policies which ultimately help the organization to decide what data to outsource, how to secure data storage and computations in various scenarios. This work also deals with the aspects of secure storage and computation in the cloud in a very distinct yet integrated manner which is a novel concept by itself. In the process, the articulation of individual user's perception about the security requirements and the trustworthiness of the CSP are captured both in terms of computation and storage and is matched with various adversarial models for final decision making at the time of outsourcing the storage and computation to the cloud.

4. REFERENCES

[1] S. De, S. Saha, and A. K. Pal, "Achieving Energy Efficiency and Security in Mobile Cloud Computing", Proceedings of the 3rd International Conference on Cloud Computing and Services Sciences CLOSER 2013, SciTePress, 8-10 May 2013, Aachen

[2] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, „Twin Clouds: An Architecture for Secure Cloud Computing", Workshop on Cryptography and Security in Clouds, 2011.

[3] Y. Chen, and R. Sion, "On Securing Untrusted Clouds with Cryptography", Proceedings of the 9th annual ACM Workshop on Privacy in Electronic Society WPES'10, ACM, New York USA, 2010, pp. 109-114.

[4] A. K. Pal and S. Bose, "Information Retrieval as a Service for Multiple Heterogeneous Data–Privacy Model", The Third International Conference on Parallel, Distributed, Grid and Cloud Computing for Engineering (PARENG 2013), Pecs, Hungary, 25-27 March 2013.

[5] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", 2nd IEEE Cloud Computing Technology and Science CloudCom, IEEE, 2010, pp. 693-702.

[6] F. Rocha, and M. Correia, "Lucy in the Sky with Diamonds: Stealing Confidential Data in the Cloud", 2011 IEEE/ IFIP 41st International Conference on Dependable Systems and Networks Workshops, 2011, pp. 129-134.

[7] R.Sandhu, and P. Samarati, "Access Control: Principle and Practice", IEEE Communications Magazine Vol. 32 Issue 9, IEEE, 1994, pp. 40-48.

[8] R. Seiger, S. Groβ, and A. Schill, "SecCSIE: A Secure Cloud Storage Integrator for Enterprises", IEEE Conference on Commerce and Enterprise Computing, IEEE, 2011.

5. AUTHOR BIOGRAPHY

Khushboo R. Shrote has received her B.Tech. degree in Computer Science and Engineering from Shri Guru Gobind Singhji institute of Engineering and Technology Nanded. Persuing her M.Tech. in Computer Science and Engineering from Government College of Engineering, Amravati, India, in 2013. Her research interest includes Data Mining, Cloud Computing.

Pushpanjali M. Chouragade has received her Diploma in Computer Science and Engineering from Government Polytechnic, Amravati, India, in 2007, the B.Tech. degree in Computer Science and Engineering from Government College of Engineering, Amravati, India in 2010 and her M.Tech. in Computer Science and Engineering from Government College of Engineering, Amravati, India, in 2013. She was a Lecturer with Department of Computer Science & Engineering, in Government College of Engineering, Amravati, in 2010-11. Her research interest includes Data Mining, Web Mining, Image Processing. At present, she is an Assistant professor with department of Computer Science and Engineering at Government College of Engineering, Amravati, India, since 2011