DATA SECURITY IN CLOUD COMPUTING

Shivali Munjal, Ramandeep Singh

Abstract -- During last few years cloud computing has been emerging from the promising business idea to the one fastest growing part of the IT industry. It is an internet based technology and one of most exciting technology of the today's world because of its scalability, flexibility and reduced cost. Cloud vendors provide services to the users on as needed basis Paas through Iaas, and SaaS. Data is stored remotely from the user's location. Therefore security and privacy are the major issues which hampers the growth of cloud because the companies have lots of data which includes audio, videos, text and digital images. The large number of solutions and methodologies has been proposed so far to protect the sensitive data. In this research, an image segmentation method is proposed for secure image partitioning for cloud services by using Optical character reader (OCR) and Cloud Analyst. With this methodology sensitive data is extracted from the non-sensitive one and then storage of sensitive data on the private cloud for security purposes is the main concept of this research study.

Index Terms— Authentication, Cloud Computing, Encryption, Migration, Optical Character Reader, Security, Segmentation

1 INTRODUCTION

CLOUD computing is one of the today's most inspiring technology in IT field. Actually cloud computing is not a new technology; it is next stage evolution of the INTERNET. You have been using cloud from long period of time, internet associated with all standards and protocols which provides all the web services to you. It is the Internet based technology where user can share resources among different cloud service providers (CSP) and cloud vendors (CV). From computing power to Computing infrastructure, business process to personal collaboration, applications all of it can be provided through the means of cloud. The set of hardware, network, storage and interface enables the delivery of computing as a service in cloud. Cloud computing is also called UTILITY-COMPUTING because it offers infrastructure to the clients on a pay as you use model by griping on the internet technology. As this model is similar to the electricity billing or water billing system so it is called as utility-computing. Cloud is made up of two essential concepts:-

1. **Abstraction:** Abstracting the system implementation details from uses and developers data locations are unknown, system administrations are outsourced to others and access by the users is ubiquitous. There is also no specification for the applications running on the physical systems.

2. **Virtualization:** Virtualization is the main concept for cloud computing. It can be achieved through pooling and sharing resources. Cost is assessed through metered basis. Scalability, elasticity and multi-tenancy are also enabled. Provisioning of system and resources from central infrastructure as needed.

- *Shivali Munjal is currently pursuing Master in Technology in Computer Science and Engineering in Lovely Professional University, India, PH-9988193713. E-mail: munjalshivalid104@gmail.com*
- *Ramandeep Singh is currently working as an assistant professor at department of Computer Science & Technology in Lovely Professional University, India, PH-9815899804. E-mail: ramankhosa@gmail.com*

2 SERVICE MODELS

2.1 Infrastructure as a service

Infrastructure as a service (Iaas) is the delivery of storage, network, server and data centre space as a service. Iaas also provides operating system and virtualization technology to its clients for managing resources. Currently, Amazon's Elastic Compute cloud (Amazon EC2) is the most high profile Iaas operation. EC2 provides web interface that allows customers to access virtual machines. It offers scalability under user's control

2.2 Platform as a service

Paas provides virtual machines, operating system, control structures, framework, and transactions. A cloud provider delivers more than infrastructure that provides everything a developer needs to build an application for both software development and runtime. Paas in multi tenant and it supports all the web services standards and delivered services with dynamic scaling. The user is responsible for installing and managing the applications that it is deploying. Google App Engine, force.com, AppJet are some of the examples of Paas.

2.3 Software as a Service

Saas is one of the first implementation of cloud service. It is the complete set of environment with application, operating system, management and user interface (UI). Application is provided to the user through browser or thin computing, its user responsibility to manage interface and data entries. CRM is one of most important category of Saas, the most prominent member in this category is salesforce.com. Google App, Window Azure, Oracle On demand are also the good examples of Saas.

.

3 SECURITY IN CLOUD

Security is the major concern for IT sector. Because of secret and confidential data in an organization which must be protected from third party or unauthorized attacks. Therefore security in cloud is the major consideration. Many levels of security are required in cloud environment.

3.1 Identity and access management

The features of IAM are authentication, authorization and auditing of the users accessing cloud services. There is trust boundary between organization which can be controlled and monitored for the applications deployed on the cloud.

3.2 Access Control-

There is need of right level of access control for the resources in the cloud environment to protect the cloud for security purpose.

3.3 Authorization and authentication-

There must be procedures and methodologies just like digital signature and encryption used in network security so that only right people can change the data or application.

4 CLOUD DATA STORAGESECURITY ISSUES IN CLOUD

The main problem cloud computing faces today is to preserve confidentiality and integrity of data. Encryption is the best solution to resolve this kind of problems. Some of the security issues are described following:

1. Trust- One of the main issue that cloud computing faces today is the trust between CSP and customers. This issue has received strong attention by companies. SLA is the only legal document which is the solution to resolve this problem which contains information of what providers is doing and willing to do.

2. **Confidentiality** It is also the major issue. Since information is stored at the remote locations and every cloud user uses the shared storage. So it is necessary to prevent the improper disclosure of information. There are many ways to prevent confidentiality but encryption is one of the main methods, however it also brings about its own issues.

3. **Authenticity (Integrity and Completeness)-** Like confidentiality, preventing integrity is also one of the main issue that needs to be handled which can only be done through encryption. There would be many users having varying accessibility rights. Some users have only rights to access the data but they might want to check the validation and completeness of results. One solution to this is to use digital signatures. But there is also a problem because not all users have access to supersets because they cannot verify the subset of data even if they are provided with digital signature.

4. Encryption- Although encryption is one the best method which provides security in cloud but it also has some drawbacks. It takes much more computational power and multiplied by many factors in database. A large amount of data is decrypted when query is run so it greatly affects the performance of database. It takes lot of time and computational power for encryption and decryption of data.

5. Key Management- Key management issue of major issue in cloud computing. In the traditional encryption techniques single is used for both encryption and decryption. But this might not be possible in case of complex problems. Customer must control and manage their key management systems because encryption keys cannot be stored on cloud. The simple systems to manage keys take the form of database which would also have secure database which is also a big problem. Now researchers developed a new method called two-level encryption which allows key management system to be stored on cloud that is somewhat efficient method.

6. **Multi-tenancy-** Storage, services, network and computational resources are shared among cloud systems to achieve better utilization and decreased cost that is called multi-tenancy. The confidentiality of data is hampered by sharing of resources. So it's very difficult to control the flow of data between these applications and make this multi-tenancy model more insecure. Virtual machines attacks and shared resources are such of issues of multi-tenancy. If there is a malicious application on one of it's which virtual server that breaches legal barriers then service providers and other authorities blocking or shutting down the servers.

5 CLOUD DATA STORAGE

Cloud storage can be implemented in many ways like local data can be backed up to cloud storage or virtual disk can be synchronized with cloud and distributed to other computers. Unlike traditional storage of FILES and BLOCKS in NAS and SAN respectively, cloud computing uses OBJECT storage. Each object is assigned its unique object ID and removing centralized indexing by using metadata along with actual data. Performance and latency interface makes object storage more suitable for backup operations. Object storage is basically used to handle unstructured data.

5.1 Key Features of Object Storage

1. Unique Object ID – Each object stored on cloud is assigned a unique object Id makes no importance to know about physical location.

2. Manage Unstructured Data- Metadata is also associated with the actual data which helps to manage any kind of data. Basically object storage in cloud is used to store unstructured data.

3. Scalability- Flat address space provides high scalability.

4. Accessibility-For Restful data and in-flight data object storage supports http and https. Web2.0 and cloud storage mandate data to be accessible over internet.

5. Cost Management- Storing data in the suitable storage tier reduces the storage cost.

6. **Data Migration-** with object ID migration of data becomes very easy in cloud.

7 PROPOSED WORK

In this research work we have gone through a lot many of papers and we have found that storage of data in cloud and its security is the major issue that the service providers face today. Manual data entry is the major problem for Indian parking vendors. For example, in many areas like traffic manage-

ment and in parking lot, all the parking vendors used to do manual entries for all the cars entered into parking. But this manual system is not efficient because it required a human being all the time to observe and note all the entries. So, we are going to propose the AUTOMATED SYSTEM for data entry.

The Main steps involves in this process are:

1. **Image Capturing:** Take the picture of the object like when we apply this system to the parking area it takes all the pictures of the cars which enters into parking with the help of digital camera.
2. **Image Segmentation:** In this step image can be segmented into two parts sensitive and non sensitive. Sensitive part contains private data like License plate, Credit card numbers etc which is very essential for users whereas non-sensitive part is not so much essential for users using OCR.
3. **Image Distribution:** Here we distribute the data among private and public cloud. This is the step which provides the security to data because we will store the sensitive data to private cloud which totally control under the service providers and having token policy which generates token for authorized users and non-sensitive data to the public cloud. So there are no chances of data loss. Moreover there is no need to save whole image over private cloud it also reduces cost and space for storing it.

This method basically takes two approaches into consideration:

1. Data Storage
2. Security

- **Data Storage:** The parking vendors in India use the manual system for data entries and store it into the cloud which is not an efficient method of storing. So we propose an automated system for data entries which automatically takes the images and stores it into the cloud only after image segmentation. The methodology uses for this image segmentation process is OCR and the tool is MATLAB. OCR (Optical Character Recognition) is a technology which is used to convert pdf or digital images into searchable or editable data [14]. Firstly OCR segments the license plate from the image of car and the extracts the characters from LP and then stores it into cloud.
- **Security:** We combine security approach with data entry process for enhancing security to the stored data entries on cloud. The extracted LP characters are the sensitive data and the remaining image is the non-sensitive part. So we stored LP characters on the private cloud for security purpose and remaining part of image on the public cloud. In the private part we use token generating approach. A token will be generated for each authorized users which can access the private cloud and can view his/her license plates stored on the cloud.

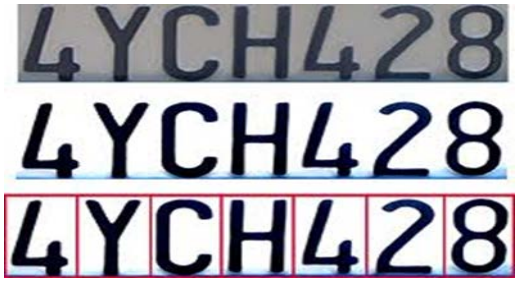

Fig1: Image Segmetatio usig OCR

8 Conclusion

In this paper, we shows that security and privacy is the main issue in cloud computing. Companies have to keep in mind before outsourcing services into cloud. Digital images contain sensitive data like credit card numbers and license plate so we must protect this sensitive data from public disclosure. In our novel approach, we present a secure image partitioning method for cloud computing which will store sensitive data on private cloud and rest of non-sensitive part on public cloud. We will give access to private cloud with the help of token only to the authorized users and public part will be accessible to anyone.

References

[1] Arulmozhi, K., Perumal, S., Siddick, A., & Nallaperumal, K. (2012). Image Enhancement Technique on Indian License Plate Localized Image for Improved Character Segmentation. *International Conference on Computational Intelligence and Computing Research* (pp. 1-6). Coimbatore: IEEE

[2] Bhisikar, P., & Sahu, A. (2013). Security in Data Storage and Transmission in Cloud Computing. IJARCSSE, 410-115

[3] Chandramohan.D, V, (2013). A privacy breach preventing and mitigation methodology for cloud service data storage. 3rd International conference on Advance Computing Conference (pp. 83-88). Ghaziabad: IEEE.

[4] Deepak Harjani, M. J. (2013). Automated Parking Management System Using License Plate Recognition. IJCTA, 741-745.

[5] Hao, F., Kodialam, M., Lakshman, T., & Puttaswamy, K. (2013). ProtectingCloud Data Using Dynamic Inline Fingerprints Checks. INFOCOM, 2013 Proceedings IEEE (pp. 2877-2885). Turin: IEEE

[6] Hojabri, M., & Rao, K. (2013). Innovation in cloud computing: Implementation of Kerberos version5in cloud computing in order to enhance the security issues. International Conference on Information Communication and Embedded Systems (ICICES), 2013 (pp. 452-456). Chennai: IEEE.

[7] Kulkarni, G., Gambhir, J., & Dongare, T. P. (2012). A security aspects in cloud computing. IEEE

[8] Lazrus, A., Choubey, S., & Sinha. (2011),"An Efficient Method of Vehicle Number Plate Detection AND Recognition, International Journal of Machine Intelligence, IJMI.

[9] N.S. Sudharshan, K. (2013). Improvising seeker satisfaction in cloud community portal: Dropbox. *International Conference on Communications and Signal Processing, 2013 (pp. 321-325). Melmaruvathur: IEEE.*

[10] Tavangarian, R. L. (2013). Secure Picture Data Partitioning for Cloud Computing Services. 27th International Conference on Advanced Information Networking and Applications Workshop (pp. 668-671). Barcelona: IEEE.

[11] V.Nirmala, R. a. (2013). Data confidentiality and integrity verification using user authenticator scheme in cloud. International conference on Green High Performance Computing (pp. 1-5). Nagercoil: IEEE.
[12] Yang, K., & Jia, X. (2013). An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. Parallel and Distributed Systems, 1717 - 1726.