ISSN:0975-9646

Enhancing Data Security and Storage in Cloud Computing Environment

Shivali Munjal[1], Shelly Garg[2]

[1]*Assistant Professor in CSE Dept, Ghubaya College of Engineering & Tech, JBD (W)*
[2]*Assistant Professor in ECE Dept, CGC COE LANDRAN*

Abstract: Cloud computing is the most emerging technology that becomes the demanding architecture for IT enterprise. A vast number of big organizations like Amazon, Google, Facebook all depends upon this type of computing. Cloud computing moves its database and applications on various data centers across various countries where management of data and its security is the major concern. A lot of services like dropbox, flickr, facebook, picasa achieved a widespread popularity for saving , organizing and managing the pictorial data which arises various security and privacy challenges. However many encryption algorithms and methodologies have been implemented yet there is no achievement over proper security. In order to achieve trust and security for picture data we represent a novel approach for secure partitioning. Basic idea behind this research is to segment and store the image on a public and private cloud to cut down the storage cost as well as protecting the user privacy by removing those attributes of the image which can be used to identify the user or the owner of the picture. For enhanced security, sensitive data is stored on the private cloud and non-sensitive data on public cloud.

Keywords: Authentication, Cloud computing, Segmentation, Optical Character Recognition (OCR), License Plate (LP), Cloud service providers (CSP), Migration, Encryption, Virtualization, Abstraction

I. Introduction

Cloud computing is one of the most inspiring technology in the IT enterprise. Actually cloud computing is the next stage evolution of the INTERNET. It is the Internet based technology where user can share resources among various Cloud vendors and Cloud service providers (CSP). It is the set of hardware, software, applications, network and interface which provides the computing as a service to its clients. Virtualization and abstraction are the two main concepts for cloud. Virtualization can be achieved through pooling and sharing of resources. Scalability, elasticity and multi-tenancy are the major features for the virtualization. Abstracting the system implementation details from the users is the major feature of abstraction. Cloud provides the various services to its clients through Infrastructure as a Service (IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS).

II. Basic Cloud Computing Architecture

A. Cloud computing service models

- **Infrastructure as a Service (IAAS):** Consumers deploy their software including OS and application on provider's infrastructure. It provides the delivery of storage, network, server and data space center as a service. Elastic Cloud Compute (EC2) provides web interface that allow consumers to access virtual machines and it is also the high profile IAAS operation.
- **Platform as a Service (PaaS):** Consumer deploy consumer created or acquired applications on the provider's created platform. The consumer doesn't manage or control the underlying cloud infrastructure including network, storage or OS but has control over the deployed applications. Google APP engine and Microsoft Window Azure are its examples.
- **Software as a Service (SaaS):** Service providers manage computing infrastructure and software to support services. Consumers use provider's applications running on their platform. EMC Mozy is an example of SaaS.

B. Deployment models

According to NIST, deployment models are categorized into four types:

Public Cloud: It is used openly by general public and situated on cloud provider's premises.

Private Cloud: It is used by single organization including many employees or business units.

Community Cloud: It is provisioned by specific community of customers having their common goals.

Hybrid Cloud: It is the combination of two or more infrastructures i.e. public, private or community.

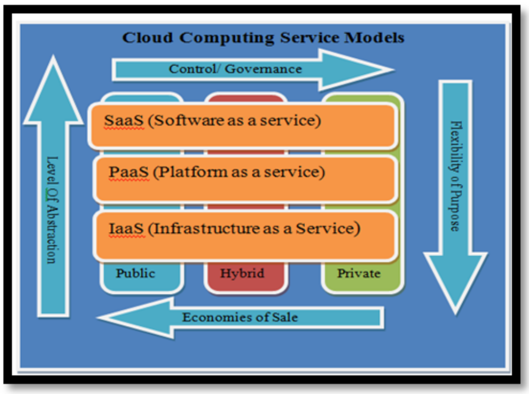
Cloud Computing Service Models
Control/ Governance
Level Of Abstraction
SaaS (Software as a service)
PaaS (Platform as a service)
IaaS (Infrastructure as a Service)
Flexibility of Purpose
Public
Hybrid
Private
Economies of Sale

Fig 1: *Deployment Model Services and Delivery*

III. Security Issues In Cloud

Security is the major concern for IT sectors to prevent the secret and confidential data from the third party. Although encryption is the best solution to prevent security yet there are various security issues

Trust: It is one of the main issues that exist between CSP and customers that achieved strong attention by the companies.

Confidentiality: Every cloud user uses the shared storage and information is stored at the remote locations. So it is necessary to prevent confidentiality by preventing the disclosure of information.

Authenticity (Integrity and completeness): It is also the main issue which can only be achieved through encryption.

Encryption: It is the best method to achieve security in cloud but it also has problem. It takes much more computational time and much more data is decrypted when query is run.

Key management: It is also the major issue because in traditional systems only single key is used for encryption and decryption. But in cloud environment customers must have to maintain their key management systems because encryptions keys cannot be stored on cloud.

Multi-tenancy: To achieve better utilization storage, network, service and computational resources are shared among cloud systems which hamper the confidentiality of data. So it's very important to control the flow of data and make the multi-tenancy model more secure.

IV. Cloud Data Storage

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.

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. **Cost Management-** Storing data in the suitable storage tier reduces the storage cost.
5. **Data Migration-** With object ID migration of data becomes very easy in cloud.

V. Challenges In Cloud Storage

- **Interoperability:** It is very difficult job to integrate all the applications because application vendors need to maintain and support extreme API's from different vendors.
- **Data Security:** To achieve proper of the stored data is the major concern because data in the cloud is accessed by various vendors and users.
- **Data Retention:** There is high data retention period in cloud because cloud is mostly used for backup and archival purpose. Since data is spanned across multiple clouds so a lot of administrative efforts are required to prevent it.
- **Portability:** Portability means cloud vendors and customers can easily move their data from one location to another. Migration of data is difficult to handle.

VI. Methodology

Through our research work we have found that storage of data and its security is the major issue that service providers face today. Preventing the pictorial data on the cloud is also very difficult because it requires sincere efforts to prevent sensitive data and its confidentiality. We implemented a AUTOMATED SYSTEM for Indian vendors which can be easily used in parking lot and toll plaza for automatic data entry for vehicles and also prevent the sensitive data for car images i.e. license plate.

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.
3) **Image Distribution:** Here we distribute the data among private and public cloud. This is the step which provides the security over data because we will store the sensitive data to private cloud which totally control under the service providers 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.

We basically take two approaches into consideration:

- Data Storage
- Data Security

Data Storage: We implemented an automated system for storing images. The methodology uses for the process is image segmentation which can be achieved through OCR i.e. Optical Character Recognition and tool used is MATLAB. Image is segmented into two parts after capturing through camera. The part of image containing the identity of user i.e. having license part is sensitive data and remaining part is non-sensitive. Sensitive part is then going to be stored in private cloud which takes very less space and remaining part on public cloud.

Data Security: Since our main concern is to secure the sensitive data. So we stored sensitive data on private cloud which is not accessible by the third party users. The user having authentication ca only enter into the private cloud.

MATLAB and Cloud Analyst are the tools that we have used to obtain the results.

Results Sets

Firstly we used the MATLAB to extract the License Plate (LP) from the whole car image. The image is firstly converted into gray scale image and the next step is edge detection because MATLAB measures the edges of the image to detect the LP from center and to extract it.

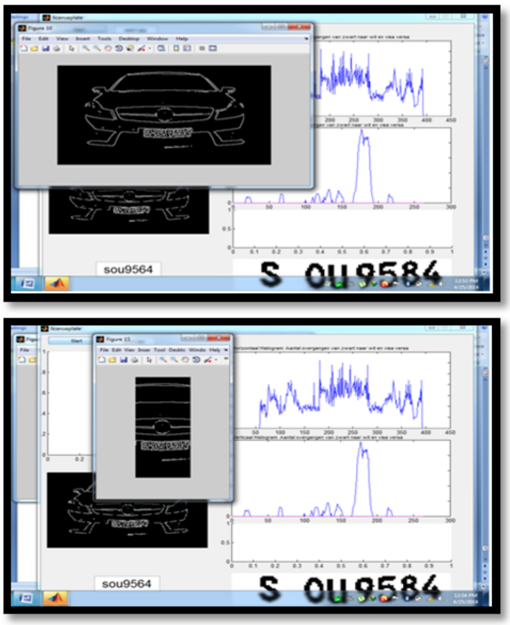

Fig 2: Gray scale image and LP extraction

Finally after extracting all the characters from the image and MATLAB matching all the characters and outliers with the image, the image is displayed without license plate.

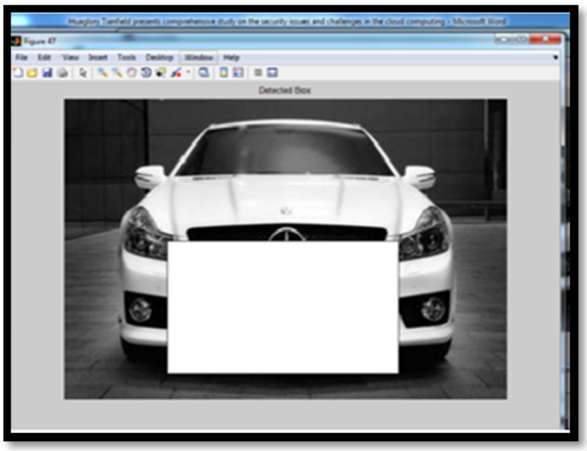

Fig3: Car image without license plate

Cloud Analyst is a simulator which provides simulation for the cloud environment. In our implemented system we used cloud analyst to store the images in the private and public cloud. In the private cloud we are going to store LP i.e. confidential part and rest of the image that is non-sensitive part in the public cloud. This system is basically designed for intelligent parking management systems for automatic entry of vehicles. When admin wants to see on what date and what time which car is entered or on particular date how many cars entered into their parking, he can easily see by using this system.

- When have two options to enter into Cloud Analyst
  - ➢ Directly into GUI
  - ➢ Through User Name and Password

Token: Token is used for security purpose. Every time one can access the private cloud it requires token. So authorized person can access the private data. When unauthorized person click on the private to see the data, he won't be able to see data.

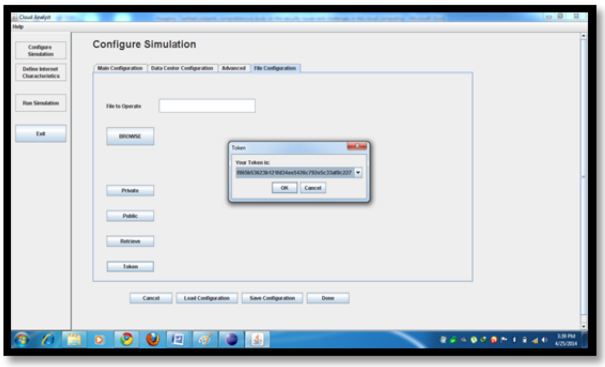

Fig4: Token to ensure security

Private Cloud: Image segmentation in itself a security method. When we are going to segment the private part of the image and going to store it in private cloud. Token is required to enter password and we can enter into the private cloud.

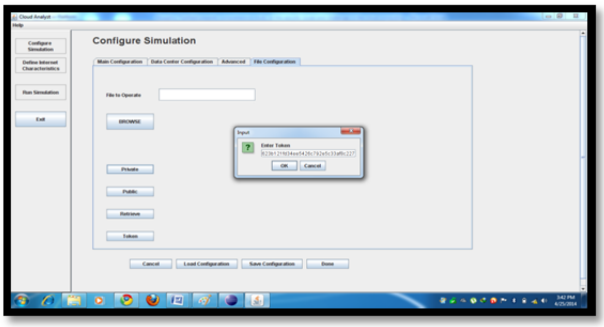

Fig5: License Plate stored in public cloud

Public Cloud: Public cloud will be accessible by anyone. There are no token or password policies. Because we are not going to store our confidential information on cloud, we need not to worry about the data present in public cloud.

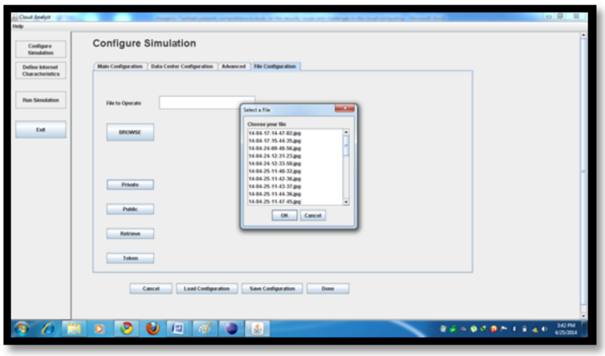

Fig7: List of images stored in public cloud

Retrieve: In the retrieve option we can fetch the License Plate number and rest of the image in parallel. It also requires password and token number because it contains the confidential data from the private cloud i.e. LP.

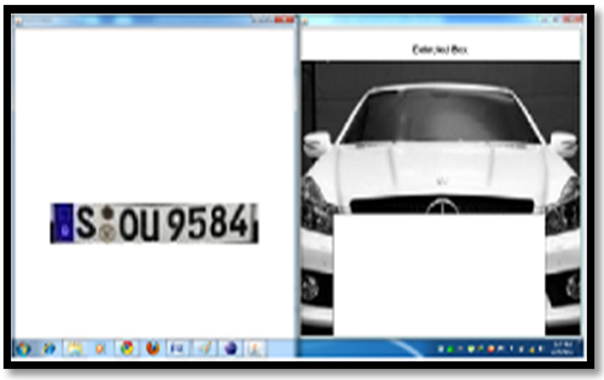

Fig8: License plate and remaining image stored at private and public cloud

VII. CONCLUSION

As the cloud Computing is emerging day by day in the today's IT world. Every organization uses cloud for storing their data. Therefore security and privacy is one of the main issues in cloud computing. As the cloud vendors provide services on the same infrastructure, so there must be some security techniques to protect the confidential data on cloud. There are lots of techniques and algorithms implemented so far yet the security breaches. We implemented a method for securing the sensitive pictorial data. This model can be easily used in electronic billing, traffic management, parking lot management and surveillance. We used the OCR for image segmentation. We extract the License Plate number from the car image that is the sensitive part of the car image. The confidential information i.e. LP on the private cloud and remaining image on the public cloud. In this way we provide the security to pictorial data of cars. This is also advantageous even the storage point of view. We can use the private cloud for storing only the small part of image rather than storing the whole image. Therefore private cloud space would be available for many more works or services.

VIII. FUTURE SCOPE

In our research and development we have used combination of MATLAB and Cloud Analytics but in future this can be done by incorporating image segmentation in a .Net application and Microsoft SQL server can be used to stored data on Microsoft Azure cloud. Also different segments of data can be encrypted with different encryption methods as per the security and privacy requirements. The other thing is that we used OCR for Image segmentation in our implemented method. Although it achieves plate extraction up to 80% which is very high rate yet we will achieve more than 90% in future by using some other tool. We will replace OCR with more efficient tool which will give the better results.

REFERENCES

[1] T. P. A. D. Gurudatt Kulkarni & Jayant Gambhir, *Security Aspects in cloud Computing*, p. 4, 2012.

[2] H. Tianfield, "Security issues in cloud computing," in *International Conference on systems, Man, and Cybernetics*, seoul, 2012.

[3] Z. Mahmood, "Data Locations and Security issues in Cloud Computing," in *Emerging Intelligent Data and Web Technologies(EIDWT)*, Tirana, 2011.

[4] A. Behl and K. Behl, "Security Paradigms for Cloud Computing," in *Computational Intelligence, Communication Systems and Networks(CICSyN)*, Phuket, 2012.

[5] B. G. L. H. L. Arjun Kumar, "Secure Storage and Access of Data in Cloud Computing," in *ICT Convergence (ICTC)*, Jeju Island, 2012.

[6] J. Wu and L. Ping, "Cloud Storage as the infrastructure of Cloud Computing," in *Intelligent Computing and Cognitive Informatics(ICICCI)*, Kuala Lumpur, 2010.

[7] P. K. I. S. K. Talasila Sasidhar, "A Generalized Storage Architecture with Backup Technology for any Cloud Storage Providers," *International Journal of Computer Applications*, pp. 256-263, 2012.

[8] P. Watson, "A multi-level security model for partioning workflows over federated clouds," *Springer*, pp. 1-15, 2012.

[9] D. Chen and H. Zhao, "Data Security and Privacy Protction issues in Cloud Computing," in *Computer Science Electronics Engineering(ICCSEE)*, Hongzhou, 2012.

[10] C. N. E.Anagnostopoulos and I. E. Anagnostopoulos, "A License Plate -Recognition Algorithm for Intelligent Transportation System Applications," *IEEE*, pp. 377-392, 2006.

[11] M. Hamdi, "Security of Cloud Computing, storage and networking," in *Collabration Technologies and Systems (CTS)*, Denver, CO, 2012.

[12] M. Zhou and R. Zhang, "Security and Privacy Issues in Cloud Cpmputing: A Survey," in *Semantics Knowledge and Grid (SKG)*, Beijing, 2010.

[13] K. N.S. Sudharshan, "Improvising seeker satisfaction in cloud community portal: Dropbox," in *International Conference on Communications and Signal Processing,2013*, Melmaruvathur, 2013.

[14] V. ,. R. ,. B. a. D. Chandramohan.D, "A privacy breach preventing and mitigation methodology for cloud service data storage," in *3rd International conference on Advance Computing Conference*, Ghaziabad, 2013.

[15] R. a. D. l. V.Nirmala, "Data confidentiality and integrity verification using user authenticator scheme in cloud," in *International conference on Green High Performance Computing*, Nagercoil, 2013.

[16] R. L. &. D. Tavangarian, "Secure Picture Data Partitioning for Cloud Computing Services," in *27th International Conference on Advanced Information Networking and Applications Workshop*, Barcelona, 2013.

[17] K. Arulmozhi, S. Perumal, A. Siddick and K. Nallaperumal, " Image Enhancement Technique On Indian License Plate Localized Image For Improved Character Segmentation," in *International Conference on Computational Intelligence and Computing Research*, Coimbatore, 2012.

[18] F. Hao, M. Kodialam, T. Lakshman and K. Puttaswamy, "ProtectingCloud Data Using Dynamic Inline Fingerprints Checks," in *INFOCOM, 2013 Proceedings IEEE*, Turin, 2013.

[19] M. Hojabri and K. Rao, "Innovation in cloud computing: Implementation of Kerberos version5in cloud computing in order to enhance the security issues," in *International Conference on Information Communication and Embedded Systems (ICICES), 2013*, Chennai, 2013.