Data Security in Cloud

Chaitanyakumar Patel
Department of Computer Science and Engineering,
Institute of Technology,
Nirma University, Ahmedabad,
Gujarat - 382481,
India

Harita Chocha
Department of Computer Science and Engineering,
Institute of Technology,
Nirma University, Ahmedabad,
Gujarat – 382481,
India

Abstract **- It is known well that cloud computing has revolutionized the field of IT enterprise through its potential advantages. Many corporations and industries are moving towards cloud computing era due to its benefits of worry-free hardware maintenance. Still large enterprises are not moving towards the cloud decreasing the amount of market size cloud computing shares. From the consumers perspective, among the various issues involved in moving towards the cloud data security and privacy issues are the major hurdles. This paper describes the various constraints related to data security and privacy protection issues as well as introduces few technologies such SecureCloud™ pioneered by Trend Micro that enables the users to operate safely and securely in cloud. Along with the personal data security on cloud using NoSQL databases.**

Index Terms – SecureCloud, FIPS 140-2, NoSQL databases, NSA, IAM policies, Accumulo Apache, Amazon DynamoDB, MarkLogic

I. INTRODUCTION

Due to advent of cheaper RAM and processors brought the client-server model into existence which in turn brought the large amount of users together sharing the same computing power on decentralized servers. Moreover bandwidth became so speedier and less costly to provide this interconnected networks to form Internet. In addition to this the hardware became so cheap allowing the cloud providers to enable the cloud technology develop through their datacenters.

More and more companies are turning towards cloud computing to provide rapid provisioning, alacrity and cost savings. Although the cloud computing services providers claims the reliability and security of their services the actual scenario is not the same. With the introduction of these new features, it gives rise to security and privacy risks. In February and July 2009, the Amazon S3 services were interrupted twice. This accident caused the lots of network based sites to be paused. In March 2009, the Google docs lead to risk the private information of its users due to vulnerability issues. Even Google's Gmail failed for about 4 hours.

Security measures of cloud computing are similar to that of traditional IT. However due to multitenant nature of cloud it faces various other risks and challenges. Though traditional measures cannot be used due to the extension of enterprise's boundaries to the cloud. Deploying the confidential information in the cloud invites the several risks and attacks due to its anonymous multi-tenant nature. Applications and storage resources stays potentially near to virtual environment causing theft risk, unauthorized exposure of information and malicious attacks. Also consumers are not guaranteed that their storage volumes will be cleared after their use. Due to this remnant data the user is at risk even after the user has vacate his/her cloud volumes. Government regulations and legislative for privacy of data also provides the additional concern for the cloud providers if data confidentiality is breached or regulated data is being moved across borders.

Here we discuss first the various issues related with the data security in brief and then introduce the Trend Micro's SecureCloud™ as one of the measures for enabling cloud users to secure their data safely and with reliability. Then we conclude with the benefits of SecureCloud™.

II. CLOUD COMPUTING SECURITY CHALLENGES

In traditional ways, enterprises put procedures and measures around their datacentres to protect their servers. Servers and hardware resources were confined within the physical boundaries so this lead to easy management of security and safety of their datacentres. Whereas in cloud computing the same approach cannot be used. Since the users data are located at remote datacentres and the users are not aware of their locations. Moreover the same datacentre holding the user's data are remotely accessed by multiple other users risking the data of users as well as the physical hardware is out of site for user with strangers.

A. Multi-Tenancy

Cloud computing consumers share the same physical hardware resources through the multi-layer software virtualization. As a result the consumers are not aware of the virtual machine next operating to it and if its intensions are to attack the hypervisor's or is looking for some malicious attacks. The consumer is totally unaware of its neighbour's identity and intentions.

Amazon Web Service security bulletin reported that the Zeus Botnet was able to install and run successfully the command and control infrastructure in the cloud environment.

B. Data Mobility and Control

Consumers put their data from static physical servers to the remote virtual servers making it dynamic and mobile allowing their data to be stored at any virtual datacentre. Also the cloud service providers make replicate copies of the data for the data maintenance and maintaining high availability. As a result comes many legal complications. As per the legislation like EU Privacy Act which forbids the residential data to be moved to the foreign datacentres. Hence the providers must ensure that such data is not being moved out of legal boundaries.

C. Data Remanence

Though recycling data is most important no standard clear methods are being designed to clear the datacentres once the consumer moves away from the cloud. Providers replicate the consumer's data at many places in order to maintain high availability and reliability but in many cases vacated hardware is being allocated to other user without being carrying out the proper recycle.

D. Data Privacy

The public nature of cloud poses an important hazard on the data privacy and confidentiality. Since the users data is located at remote virtual place there is always the risk of data breaches and heavy fines are to be paid by the offending company for that. Also it causes business loss impacts and also personal level loss in case the confidential medical records are exposed.

III. SOLVING THE CLOUD SECURITY CHALLENGE

Trend Micro's SecureCloud™ [1] provides the distinctive feature of data protection and security to cloud and virtual environments using encryption with policy-based key management and unique server validation. It allows the business to operate securely with sensitive data in the public cloud with providers such as Amazon EC2, Dell, Eucalyptus, and NTT America, as well as VMware vCloud and any virtual environment.

Some of the key features of the SecureCloud™ are:

1) *Advanced Security Techniques*
   a) Features Federal Information Processing Standard (FIPS) 140-2 [2] certification and Federal Information Processing Standard (FIPS) approved Advanced Encryption Standard (AES) encryption [3].
   b) Encrypts and decrypts information in real time, so data at rest is always protected.
   c) Applies whole volume encryption to secure all data, metadata, and associated structures without impacting application functionality.

2) *Access and Authentication Controls*
   a) Employs role-based management to help ensure proper separation of duties.
   b) Automates key release and virtual machine authorization for rapid operations or requires manual approval for increased security.
   c) Offers cloud provider credential rotation.

3) *Policy-driven Key Management*
   a) Uses identity- and integrity-based policy enforcement to ensure only authorized virtual machines receive keys and access secure volumes.
   b) Integrates with Deep Security Manager to further validate the environment security posture.
   c) Enables the use of policies to determine when and where information is accessed.

4) *Robust Auditing, Reporting, and Alerting*
   a) Logs actions in the management console for audit purposes
   b) Provides detailed reporting and alerting features with incident-based and interval based notifications

Trend Micro's SecureCloud™ offers following functionalities to its users that helps to secure their data on cloud.

A. Easy Deployment

SecureCloud™ ensures that the data stored in the cloud is protected through the encryption at the kernel level with a simple agent being installed in the virtual image. This avoids the any man-in-middle attacks to gain access to the encryption keys as the communication between this agent and the SecureCloud™ is secure.

B. Secure Key Management

In SecureCloud™ consumers have the exclusive access to the encryption keys and hence total control over their data as well. The encryption key management is done by the consumers or the Trend Micro but not by the cloud providers. This provides the cloud consumers to have benefits of the cloud facilities as well as have the total control over their data through encryption keys.

VM-level encryption used by the SecureCloud™ provides the encryption of the data in the working storage allowing different encryption keys for different information of various consumers. This mitigates the risk of allocating the recycled disk blocks to other consumers or to fall victim of error configuration which would compromise the data privacy.

C. Industry Standard Encryption

Industry Standard AES encryption used by SecureCloud™ makes the data unreadable and useless for the one without the encryption keys. SecureCloud™'s feature of encrypting the data allows the consumers to have benefits when changing users or terminating storage. Any encrypted data remaining on the storage is unrecognizable and useless making it secure for the consumers. This reduces the risks to data theft, exposure to unauthorized parties etc.

D. Granular Control

User gets to know exactly which server gets access to its encrypted data through SecureCloud™'s unique policy based key management and secure data access. Virtual servers must first authenticate the SecureCloud™'s key server with credentials that have been encrypted in the virtual machine's kernel. Based on the defined policies the SecureCloud™'s key server checks the information and releases the key to the server if approved to be harmless virtual environment. Also it provides the role based access to the administrators with specific permission levels from full access, key access to audit logging.

E. Custody of Encryption Keys

Users are provided with the control data access of isolating the physical key storage from the cloud infrastructure provider. This stops the infrastructure provider from accessing the keys and giving full control to the consumers to move from one vendor to another avoiding the vendor lock-in problem. It's on premise solution gives more facilities by allowing the keys to be stored in the SecureCloud™'s custody all the times.

F. Reporting

SecureCloud™'s allows to view the system configuration settings through audit trail of key approvals on the management server. It also allows the detailed logging and reporting for any actions performed for key approvals. All changes coming from the administrator's or the system itself are also logged and monitored.

IV. NoSQL DATABASES

As a cloud user we can't make sure about the security of confidential information. Since the cloud provider also cannot provide 100% guarantee in the safety. In such scenarios NoSQL databases [4] become a popular choice working with large data sets. Now, big data administrators can leverage the benefits of NoSQL and still maintain some control over who can access subsets of data in the cloud.

There are three different ways to secure NoSQL data stores:

- Accumulo's cell-based access controls [5]
- Amazon DynamoDB [6] use of Amazon Web Services (AWS) Identity and Access Management (IAM) [7] policies
- MarkLogic's [8] compartment controls and execute privileges.

A. Accumulo Data Store

A distributed, key value data store based on Google's Big Table. Created by the NSA and releases in 2011. Accumulo is an Apache project and runs on the Hadoop environment, with additional features not found in Big Table, including cell-based access controls.

Accumulo keys include a visibility attribute that specifies security labels, such as admin, finance or manager. Because each key is associated with a single value, the equivalent of a row in a relational table, key-based access controls limit the set of rows that a user can query or manipulate. Users are then assigned authorizations that specify certain security labels, which can be combined in logical expressions to create access controls as needed. For example, a manager in the finance department would be assigned both the "manager" and "finance" labels.

B. Amazon DynamoDB

DynamoDB is a key-value data store service that provides automated scalability and provisioned IOPS. Amazon DynamoDB is a good option for developers and application managers who prefer a hosted service to administering their own NoSQL database.

To maintain fine-grained access control in Amazon DynamoDB, admins must specify conditions in an IAM policy. Conditions allow or deny access to particular items and attributes in the key-value data store. This model limits access to particular values or rows, such as data associated with a particular customer account so customers can only see their data.

C. MarkLogic

Document-based NoSQL databases, such as MarkLogic, can extend role-based access controls to group roles and documents into compartments. MarkLogic also provides access control over the execution of operations. The database includes a set of predefined execute privileges that deal with data management, security and other administration operations.

V. CONCLUSION

Despite the various avenues provided by cloud computing, data security and safety always arises. Some of the cloud providers use encryption, key management and various techniques to tackle this risk.

Trend Micro's SecureCloud™ allows the user's to move their data in virtualized environment without any data security issues through its encryption and patented key management. It protects and maintains the user's data thus providing the user the flexibility to move between the cloud users, having full control over their data and deciding whom to give access. It provides the complete solution for safeguarding information in private cloud as well as public infrastructure-as-a-service.

Some enterprises and IT managers of cloud employ NoSQL database policies to secure the data on cloud and restricting the access using appropriate queries, privileges and

table compartments. For example Accumulo's cell-based access controls, Amazon DynamoDB, MarkLogic's compartment control.

V. REFERENCES

[1]. http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_SecureCloud.pdf
[2]. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[3]. http://cmpe.emu.edu.tr/Courses/CMPE553/Notes/Ch5.AES.doc
[4]. http://searchcloudcomputing.techtarget.com/tip/Amazon-DynamoDB-Accumulo-access-controls-secure-big-data-in-the-cloud
[5]. https://accumulo.apache.org/1.5/accumulo_user_manual.html
[6]. http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html
[7]. http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html
[8]. http://docs.marklogic.com/