International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 608-611 1 May 2014

Security Enhancement on Cloud using Multi Cloud Concepts

[1]Dhayalan.D, [2]Saravanan.M
Veltech Multitech Dr.Rr Dr.Sr Engineering College
[1]dayalan.moorthy@rediffmail.com [2]saravanan.techone@gmail.com

Abstract—***security challenges are still among the biggest challenges or obstacles in the field of cloud computing and services. Many research activities are done in clearing those issues. In this journal we concentrated on security issues by involving multi cloud architectures and introducing a concept called database splitting which can enable security.***

Keywords—cloud, multi cloud, database splitting, partitioning, cryptography, encryption.

Introduction

Cloud computing provide dynamically usable and large resources provisioned as a service over the web. The third party, pay-per-use, and seamlessly large and usable computing resources and services offered by the cloud paradigm promise to reduce capital amount as well as operational cost for hardware and software. Clouds can be categorized by taking the physical location into account from the viewpoint of the cloud user. A public cloud is offered by the third-party service providers and involves resources outside the user's system. In case the cloud system Is installed on the user's system in the own data center—this setup is called private cloud. A hybrid approach is denoted as hybrid cloud

Major idea on reducing the risk for data and applications in saving in a public cloud is the distinct usage of multiple clouds. Many approaches employing this style or concept have been proposed recently. They differ in separating or distribution patterns, secure technologies, cryptographic methods, and at security levels. This journal paperis an extension and contains a survey on these different security issues by multi cloud adoption approaches. These multi cloud architectures allow to categorize the available methods
analyze them according to their security benefits.
An assessment and survey of the different methods with regards to legal aspects.
The rest of this paper is organized as follows:
The second section motivates and explains about the need for effective and proper cloud security counter measures by completely examining the current security levels. The current research work are done basically on the part of security and not on the part of the cloud itself. After the start of research in multiple clouds the importance of cloud concepts are being taken into research.

Issues in Cloud security:

In cloud computing there are large number of security issues and challenges. The issues ranges from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem is that of secure outsourcing of sensitive as well as business-critical data and processes.
An hacker or an attacker who has access to the cloud storage materials is able to alter data in the storage. An hacker or an attacker also has large access to the operating logic of the cloud and can dominantly can able to modify the input and output data. Even though in many cases it is possible to assume that a cloud provider is very honest in handling the customer in a respectful manner and in a secure manner but still there are malicious workers of the cloud provider who successfully attacks and damage the data under the supervision of third party persons. Database splitting is another way of securing the data and will be discussed briefly.
Some examples of attacks are Ristenpart et al.had given some attack techniques for the virtualization of the Amazon IaaS service. In their
approach, the hacker allocates new virtual machines until one works on the same physical machine as the victim's machine.

II. Material and Methodology

SECURITY PROSPECTS BY MULTICLOUD ARCHITECTURES
The basic idea is to use multiple distinct clouds to vanish or overcome the risks of malicious data manipulation, and disruptions in processes. By integrating many distinct clouds, the trust assumption can be lowered to an assumption of non collaborating cloud service providers. By introducing multi cloud it makes much harder for an external attacker to retrieve or damage the hosted data or applications of a particular cloud user. The idea of making use of multiple clouds has been proposed by Bernstein and Celesti .Many security techniques and methods are adopted to solve the issues in the cloud. In multi cloud, cryptographic methods such as encryption and decryption and key management are used. Database splitting is one of the other important security technique in involving a multi cloud.

FOUR MAJOR PART OF MULTI CLOUD ARCHITECTURE:

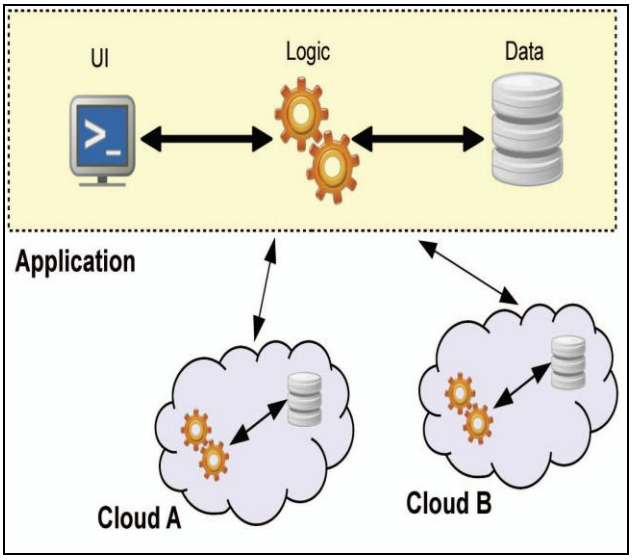
Integrity of applications : it allows to receive multiple results from one operation performed in multiple clouds and to compare them within the own premise. This gives the user to get an view on the integrity of the result.

Segregation of application System into tiers allows to segregate the logic from the data This enables extra
protection against data damage due to problems in the application logic
.
Segregation of application logic into fragments allows sending the application logic to distinct clouds
This has two important usage benefits. The two advantages are no cloud service provider learns the complete application logic. Second, no cloud service provider identifies the overall output of the application. Thus, this makes the data and application to be in the safer level

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 608-611 1 May 2014

Segregation of application data into fragments allows sending finely segregated fragments of the data to distinct multiple clouds. None of the cloud service providers gains access to all the data, which makes the data safer.The coming Figure explains about segregation of logics and data and storing it in multiple clouds.

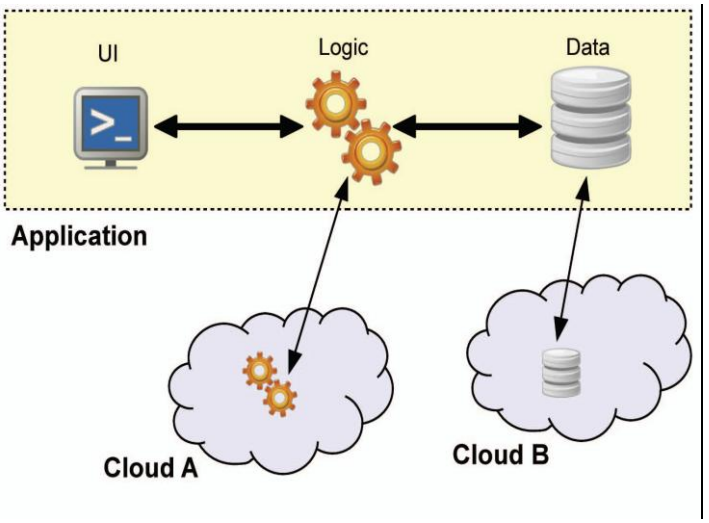
Segregating both logics and data:



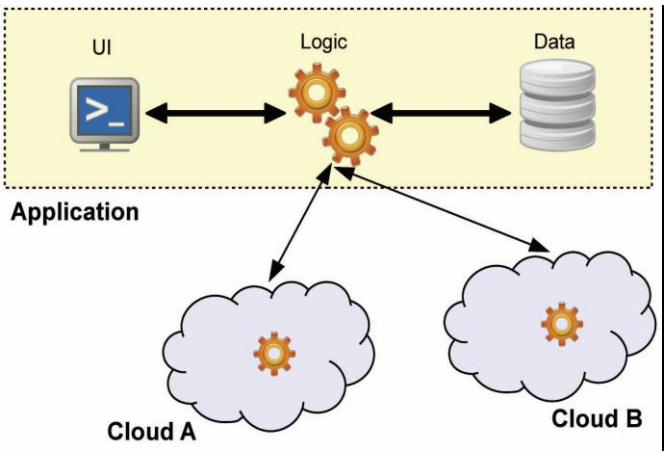
Separation of application logic into number of fragments: Security issue in a cloud is very difficult to eradicate and control but it can be controlled by using distinct multiple clouds. In multicloud separation can be done in many ways, one of the way is that the logic of the application or data can be divided to the different levels and send it to different cloud providers. In this method we can divide the data into different parts, and in this process of division one critical share of data can be sent to a trusted private cloud service provider. The other small parts can be stored in some untrusted service providers assuming that the datas are safe and does not collude.

Encryption and multi party computation:
Encryption and multiparty computation means securing it while it is processed. In this encryption part of the multi cloud concept the user can encrypt the data with his public key and uploads the cipher text into the cloud. In this method the cloud provider is independently encrypts the data and only the particular user can decrypt it.

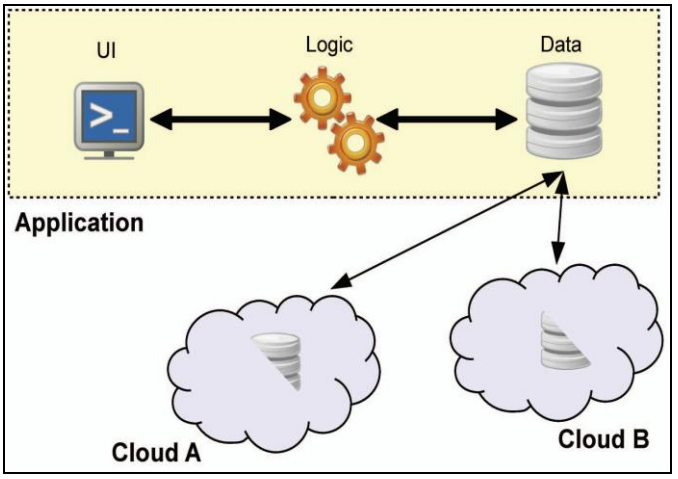
Segregation of application system into tiers:



Segregation of application logic into fragments:



Segregation of application data into fragments:



III. Results and Tables
Database splitting

For protecting information inside databases, we have to provide two security goals: confidentiality of data items or confidentiality of data item relationships. In the first case, data splitting requires a scenario similar to other approaches presented before with a least one trusted cloud provider. However, very often only the relationship can be protected, and this can be achieved using just proper and secured providers.

For splitting a database table, there are two general approaches: Vertical fragmentation and horizontal fragmentation. With vertical fragmentation, the columns are distributed to cloud providers in such a way that no single provider learns a confidential relationship by his own. For example, A patient health record, might be fragmented into two parts. This way, the individual providers only learn noncritical data relations. However, it is a nontrivial task to find such a fragmentation. First, new relations can be found by performing different combination of existing ones. some relations can be concluded using outside experience and knowledge. If, in the example above, even if the first provider additionally learns about the connection, he has technically still no knowledge about the patient's disease. However, someone with knowledge in pharmaceutical background can derive the disease from the medication.

Data Splitting using cryptography:

The most basic cryptographic method to store data securely is to store the data in encrypted form. While the cryptographic key or the cipher key could remain at the user's premises, to increase trust and flexibility in cloud data processing or to enable multiuser systems it is beneficial to have the key available online when needed. This approach, distributes key material and encrypted data into different clouds. A similar approach is taken by many solutions for secure cloud storage: The first approach to cryptographic cloud storage is a solution for encrypted key/value storage in the cloud while maintaining the ability to easily access the data. It involves searchable encryption as the key component to achieve this. Searchable encryption allows keyword search on encrypted data if an authorized token for the keyword is provided.

Database tables creation

```
CREATE TABLE `private_cloud1` (
  `id` int(11) default NULL,
  `name` varchar(255) default NULL,
  `tname` varchar(255) default NULL,
  `signature` varchar(255) default NULL,
  `master_key` varchar(255) default NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- ----------------------------
-- Table structure for profile
-- ----------------------------
DROP TABLE IF EXISTS `profile`;
CREATE TABLE `profile` (
  `id` int(255) default NULL,
  `name` varchar(255) default NULL,
  `email` varchar(255) default NULL,
  `password` varchar(255) default NULL,
  `gender` varchar(255) default NULL,
  `location` varchar(255) default NULL,
  `date` varchar(255) default NULL,
  `prime` varchar(255) default NULL,
  `generator` varchar(255) default NULL,
  `privatekey` varchar(255) default NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- ----------------------------
-- Table structure for public_cloud2
-- ----------------------------
DROP TABLE IF EXISTS `public_cloud2`;
CREATE TABLE `public_cloud2` (
  `id` int(11) default NULL,
  `age` varchar(255) default NULL,
  `disease` varchar(255) default NULL,
  `stage` varchar(255) default NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- ----------------------------
-- Table structure for public_cloud3
-- ----------------------------
DROP TABLE IF EXISTS `public_cloud3`;
CREATE TABLE `public_cloud3` (
  `id` int(11) default NULL,
  `drug` varchar(255) default NULL,
  `location` varchar(255) default NULL,
  `message` varchar(255) default NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- ----------------------------
-- Table structure for single_cloud
-- ----------------------------
DROP TABLE IF EXISTS `single_cloud`;
CREATE TABLE `single_cloud` (
  `id` int(11) default NULL,
  `name` varchar(255) default NULL,
  `tname` varchar(255) default NULL,
  `age` varchar(255) default NULL,
  `disease` varchar(255) default NULL,
  `stage` varchar(255) default NULL,
  `drug` varchar(255) default NULL,
  `location` varchar(255) default NULL,
  `message` varchar(255) default NULL,
  `public_key` varchar(255) default NULL,
  `master_key` varchar(255) default NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- ----------------------------
-- Records
-- ----------------------------
INSERT INTO `private_cloud1` VALUES ('101', 'kutty', 'sweety', '8784635503676414861', '/./3');
INSERT INTO `private_cloud1` VALUES ('102', 'alice', 'bob', '5209890786700379649', '135-');
 INSERT INTO `profile` VALUES ('1', 'kutty', 'kutty@gmail.com', 'kutty', 'male', 'Chennai', '11-01-2014', '13170289529977551289', '2', '544');
INSERT INTO `profile` VALUES ('2', 'sweety', 'sweety@gmail.com', 'sweety', 'female', 'Chennai', '11-01-2014', '18348213115544407231', '2', '252');
INSERT INTO `profile` VALUES ('3', 'alice', 'alice@gmail.com', 'alice', 'male', 'Bangalore', '11-01-2014', '12954686100061351979', '1', '263');
```

INSERT INTO `profile` VALUES ('4', 'bob', 'bob@gmail.com', 'bob', 'female', 'Bangalore', '11-01-2014', '14394460658037444947', '1', '619');
INSERT INTO `public_cloud2` VALUES ('96', 'XXX', 'XXX', 'XXX');
INSERT INTO `public_cloud2` VALUES ('97', 'XXX', 'XXX', 'XXX');
INSERT INTO `public_cloud2` VALUES ('98', 'XXX', 'XXX', 'XXX');
INSERT INTO `public_cloud2` VALUES ('99', 'XXX', 'XXX', 'Middle');
INSERT INTO `public_cloud2` VALUES ('100', 'XXX', 'Cancer', 'Starting');
INSERT INTO `public_cloud2` VALUES ('101', '28', 'Aids', 'XXX');
INSERT INTO `public_cloud2` VALUES ('102', '25', 'XXX', 'XXX');
INSERT INTO `public_cloud3` VALUES ('96', 'XXX', 'XXX', 'XXX');
INSERT INTO `public_cloud3` VALUES ('97', 'XXX', 'XXX', 'XXX');
INSERT INTO `public_cloud3` VALUES ('98', 'XXX', 'XXX', 'XXX');
INSERT INTO `public_cloud3` VALUES ('99', 'XXX', 'XXX', 'Hello doctor , i am suffering from cancer.');
INSERT INTO `public_cloud3` VALUES ('100', 'XXX', 'Chennai', 'Hi doctor, see my details.');
INSERT INTO `public_cloud3` VALUES ('101', 'Anacine', 'Bangalore', 'XXX');
INSERT INTO `public_cloud3` VALUES ('102', 'Metacino', 'XXX', 'XXX');
INSERT INTO `single_cloud` VALUES ('101', 'kutty', 'sweety', '28', 'Cancer', 'Middle', 'Anacine', 'Chennai', 'Hello doctor , i am suffering from cancer.', '8784635503676414861', '/./3');
INSERT INTO `single_cloud` VALUES ('102', 'alice', 'bob', '25', 'Aids', 'Starting', 'Metacino', 'Bangalore', 'Hi doctor, see my details.', '5209890786700379649', '135-');

CONCLUSION

The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. As the approaches investigated in this paper clearly show, there is no single optimal approach to foster both security and legal compliance in an omni applicable manner. Moreover, the approaches that are favorable from a technical perspective appear less appealing from a regulatory point of view, and vice versa. The few approaches that score sufficiently in both these dimensions lack versatility and ease of use, hence can be used in very rare circumstances only.

Database splitting is an important menthod to secure data which can be enabled in a multi cloud architecture.

As can be seen from the discussions of the four major multicloud approaches, each of them has its pitfalls and weak spots, either in terms of security guarantees, in terms of compliance to legal obligations, or in terms of feasibility. Given that every type of multicloud approach falls into one of these four categories, this implies a state of the art that is somewhat dissatisfying.

ACKNOWLEDGMENTS

The work of Meiko Jensen and Ninja Marnau was fundedby the European Commission, FP7 ICT Program, Contract 257243 (TClouds Project).

REFERENCES

i. *P. Mell and T. Grance, "The NIST Definition of Cloud Computing,Version 15," Nat'l Inst. of Standards and Technology, Information Technology Laboratory, vol. 53, p. 50, http://csrc.nist.gov/groups/SNS/cloud-computing/, 2010.*

ii. *F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits&Challenges,"blog, http://blogs.idc.com/ie/?p=210, 2008.*

iii. *Gartner, "Gartner Says Cloud Adoption in Europe WillTrailU.S.byatLeastTwoYears," http://www.gartner.com/it/page.jsp?id=2032215, May 2012.*

iv. *J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono,"Security Prospects through Cloud Computing by AdoptingMultiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing(CLOUD), 2011.*

v. *D. Hubbard and M. Sutton, "Top Threats to Cloud ComputingV1.0," Cloud Security Alliance, http://www.cloudsecurityalliance.org/topthreats, 2010.*

vi. *M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," Proc. IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.*

vii. *T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You,Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer andComm. Security (CCS '09), pp. 199-212, 2009.*

viii. *Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VMSide Channels and Their Use to Extract Private Keys," Proc. ACMConf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.*

ix. *N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," Proc. IEEE Int'l Conf. Web Services (ICWS '09), 2009.*

x. *M. McIntosh and P. Austel, "XML Signature Element WrappingAttacks and Countermeasures," Proc. Workshop Secure WebServices, pp. 20-27, 2005.*