DATA SCAVENGING THREAT IN CLOUD COMPUTING

[1]SHILPI CHANDNA, [2]ROHIT SINGH, [3]FAZIL AKHTAR

[1]Career Point University, Kota; [2]Career Point University, Kota; [3]MAIIT, Kota
E-mail: schandna23@gmail.com, rohitsingh051@gmail.com, akhtar.fazil@gmail.com

Abstract- Cloud computing is a web based technology that change our way of working and provide online collaboration. Cloud computing is user centric, task centric, powerful, accessible, intelligent and programmable. Cloud computing offers convenience, speed, provides users with on – demand services and can be accessed when required. Several benefits are offered by cloud computing but one of the barrier of cloud computing is security because data is stored on multiple third-party servers, rather than on the traditional dedicated servers which are used in traditional data storage. Cloud computing can be broken down into three distinct layers offering different service types known as SPI model. This paper describes the threats found in the SPI model. Countermeasures for various threats such as data leakage, customer-data manipulation VM escape, malicious VM creation, insecure VM migration, sniffing/spoofing virtual networks have been provided but countermeasures for denial of Service, VM hopping and data scavenging are not provided. Countermeasure for data scavenging is provided in this paper.

Keywords- SPI model, Cloud computing, Threats, Security

I. INTRODUCTION

Cloud computing is a general term which is useful for describing a new class of network based computing which takes place over the Internet. In cloud computing, applications and files are hosted on a "cloud" which consists of thousands of computers and servers, which are all inked together and accessible via the Internet.With cloud computing, we can access all our applications and documents from anywhere in the world, freeing us from the confines of the desktop, everything is now web based instead of desktop based. Cloud computing is one of the fastest growing segments of the IT industry. In Cloud computing, security controls are, for the most part no different than security controls in any IT environment. But, because of the cloud services models, operational model and the technologies used to enable cloud services, different risks are presented by Cloud computing to an organization than traditional IT solution. Authentication, identity and authorization, the traditional security mechanisms are no longer enough for clouds. Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model is composed of three layers: SaaS, PaaS, and IaaS which is known as SPI model shown in fig.1.

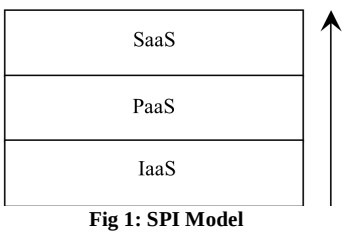

Fig 1: SPI Model

One of the major issues which reduce the cloud computing growth is security. Cloud computing offers several benefits but one of the barrier of cloud computing is security which is followed by issues regarding legal matters, compliance and privacy. Risk areas of cloud relate to security including external data storage, lack of control, multi-tenancy. The cloud has many features such as its large scale and resources belonging to cloud providers are heterogeneous, virtualized and distributed. Cloud computing offers a risk because third party provider who owns the infrastructure delivers the Cloud computing services.

Here Security issues for cloud computing are focused on SPI model identifying threats related to Cloud computing. For all layers of cloud, identification and assessment of threats is an important pre- cursor in order to understand and identify the risk.

Cloud computing services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

1.1 Infrastructure-as-a-Service (IaaS)

It provide capability to consumer to provision processing, networks, storage and other fundamental computing resources where the consumer is able to run and deploy arbitrary software . It is the delivery of computer infrastructure as a service. Customers buy fully outsourced service rather than purchasing software, servers, data center space or network equipment.

1.2 Platform-as-a-Service (PaaS)

Customer is able to deploy on the cloud his own applications without installing any tools or platform on their local system. It provides platform layer

resources including software development framework and operating system support.

1.3 Software-as-a-Service (SaaS)

Customer is provided with the capability to use provider's applications which are running on the cloud infrastructure. Clients can access the applications through thin client interface such as web browser.

The burden of security lies with the cloud provider in case of SaaS. The SaaS model is based on a high degree of integrated functionality with minimal consumer control. But PaaS offer greater consumer control and extensibility. IaaS offer greater tenant control because of lower degree of abstraction than PaaS or SaaS.

We need to understand the relationships and dependencies between SPI models to analyze security challenges in Cloud Computing. On the top of IaaS, PaaS and SaaS are hosted which is shown in fig1. Thus any problem in IaaS will affect both SaaS and PaaS as well.

II. ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

A weakness in a system which can be exploited by a threat is the vulnerability. By reducing the vulnerability aspect of the system, we can reduce the risk and impact of the threats. Many existing technologies such as web browsers, virtualization and web services contribute to the evolution of cloud environment. Thus, any vulnerability associated with this technology will also affect the cloud.

Data storage and virtualization are most critical and an attack to them can perform the maximum harm. Table 1 shows the threats, their countermeasures and the layers to which they belong. This paper gives emphasis on the data scavenging threats associated with data being stored and processed remotely. The technique of piecing together information which is found from bits of data is data scavenging. Since data cannot be completely deleted, an attacker can recover the data. This is known as data scavenging. Data scavenging attacks are of two types:

- Keyboard attack: These are the attacks through resource which are available to the normal system users who are sitting at the keyboard.
- Laboratory attack: This is through precise electronic equipment; these attacks are planned, orchestrated attacks.

Countermeasures

Countermeasures for various threats except data scavenging, VM hopping and denial of service are discussed below.

2.1 Countermeasures for Data Leakage

2.1.1 Digital signatures

Digital signatures, a form of electronic signatures, are created and modified using public key cryptography that is based on the concept of a key pair generated by a mathematical algorithm, public and private.

2.1.2 Fragmentation-redundancy-scattering (FRS) technique

In this technique, sensitive data is broken into insignificant fragments so that any fragment does not have any significant information by itself. Fragments are then scattered across different sites. This technique provides intrusion tolerance and thus secure storage.

2.1.3 Homomorphic encryption

It allows performing arbitrary computation on cipher texts without being decrypted. Limited number of homomorphic operations such as addition and multiplication are supported by current homomorphic encryption.

TABLE 1: THREATS IN CLOUD COMPUTING

SN	Threat	Countermeasures	Layer
1	Data Leakage	Digital Signature FRS Technique Homomorphic encryption Encryption	SPI
2	Service or Account Hijacking	Identity and Access Management guidance Dynamic Credential	SPI
3	Customer Data Manipulation	Web application scanners	S
4	VM escape	TCCP TVDc HyperSafe	I
5	Malicious VM creation	Mirage	I
6	Insecure VM migration	PALM VNSS	I
7	Sniffing / Spoofing virtual network	Virtual network security	I
8	Data Scavenging	Symmetric key Cryptography	SPI
9	Denial of Services	Policies can be offer by cloud providers.	SPI
10	VM Hopping	-	I

2.1.4 Encryption

Sensitive data is secured with Encryption techniques. By sending or storing encrypted data in the cloud, it is ensure that data is secure. AES scheme is one of the well known encryption algorithm. To protect data while it is in transit, SSL technology can also be used.

2.2 Countermeasures for Account or Service Hijacking

2.2.1 Identity and access management guidance

Identity management includes creation, management and removal of a digital identity. Access management includes authorization of access to only the data an entity needs to access to perform required duties efficiently and effectively. Identity and access management guidance provide best practices to assure secure access management and identity.

2.2.22.2.2 Dynamic credentials

In this, user sets the password and user name on a screen which is pointed to by the credential request starting point. The text field must have corresponding credential cache user name and password checkbox which is checked to indicate the value which is to be used to provide password and user name on the client.

2.3 Countermeasures for Customer Data Manipulation

2.3.1 Web application scanners

Web applications are easy target because of exposure to public including potential attackers. In order to identify security vulnerability web applications are scans through the web front–end. Other web applications security tools include web application firewall.

2.4 Countermeasures for VM escape

2.4.1 Trusted cloud computing platform

Trusted cloud computing platform enables IaaS providers to provide a closed box execution environment which guarantees confidential execution of guest virtual machine.

2.4.2 Trusted Virtual Datacenter

Isolation and integrity in cloud environment is provided by Trusted Virtual Datacenter. Datacenter is a home to the computational power and storage is central to cloud computing and contains thousands of devices like servers, switches and router.

2.4.3 HyperSafe

HyperSafe is a light weight approach to provide lifetime hypervisor control-flow integrity. HyperSafe goal is to protect hypervisor using two techniques, non- by passable memory lockdown and restricted pointer indexing. Non- by passable memory lockdown protects the hypervisor's code and static data from being compromised and restricted pointer indexing convert the control data into pointer indexes.

2.5 Countermeasures for Malicious Virtual Machine Creation

2.5.1 Mirage

For constructing secure, high performance network applications, mirage is a unikernel across cloud computing mobile platforms. Unikernel is a new approach in order to deploy cloud services via applications which are written in high level source code.

2.6 Countermeasures for Insecure Virtual Machine Migration

2.6.1 Protection aegis for live migration of VMs (PALM)

It preserves privacy protection and integrity during and after migration. The prototype was implemented based on GNU Linux and Xen.

2.6.2 VNSS

VNSS provides continuous protection through virtual machine live migration. A prototype based on Xen and GNU Linux is implemented.

2.7 Countermeasures for Sniffing/Spoofing Virtual Networks

2.7.1 Virtual network security Communication among virtual machine is secure through virtual network framework which is based on Xen offering two configuration modes for virtual networks, that is, bridged and routed. VMs can be protected from sniffing and spoofing by this virtual network model which consists of three layers: routing layers, shared network and firewall.

III. PROPOSED SCHEME

Data storage is one of the primary use of cloud computing. With cloud storage, data is stored on multiple third- party servers, rather than on the traditional dedicated servers which are used in traditional data storage. The user sees a virtual server, when storing data. It seems that data is stored on some particular place with a particular name but that place does not exist in reality. But, actually user data may be stored on any one or more computers which are used to create a cloud. As the cloud dynamically manages available storage space, therefore, actual storage location of user data may vary from day to day or even from minute to minute. The user sees static location of his data even though the location is virtual.

We can secure the data on the cloud by encrypting the data before it is stored on the cloud. In the proposed scheme, we have use the secret key cryptography consisting of the technique known as password authentication. The flowchart for the proposed scheme is shown in fig 2.

Our proposed scheme consists of two algorithms, one for uploading the file and another one for restoring deleted file from cloud sever.

The algorithm for uploading a file is as follows:

Step 1 The file is created with the name 'Default'.

Step 2 Parameter = object sender, EventArgs e

/* Page is loaded along with above parameters. */

Step 3 Parameter = object sender, EventArgs.

Event=Click

/* 'Save' button is created with above parameters */

Step 4 Now we will check to see if file was uploaded.

Step 5 Get a reference to Posted File object.

Step 6 Get size of uploaded file.

Step 7 if (nFileLen>0)

/* Make sure that the size of the file is greater than zero. */

Step 8 Set Allo= Read File

/*Allocate a buffer for reading of the file.*/

Step 9 Read uploaded file from the Stream zero to n.

Step 10Set the path for the file set in step 10.

Step 11Write data into a file set in step 10.

Step 12Use Path class to manipulate file and directory paths.

Step 13Through 'input and output command', we can copy the file to another location and overwrite the destination file if it already exists.

Step 14Parameter = SourceFile, DestFile

/ *To perform encryption, file is created with the name 'EncryptFile' having above parameters. */

Step 15String password='*********'

/*After the file creation, we got the file in the form of bytes using the above password.*/

Step 16 Object= fscrypt

/* Filestream is call by the above object . */

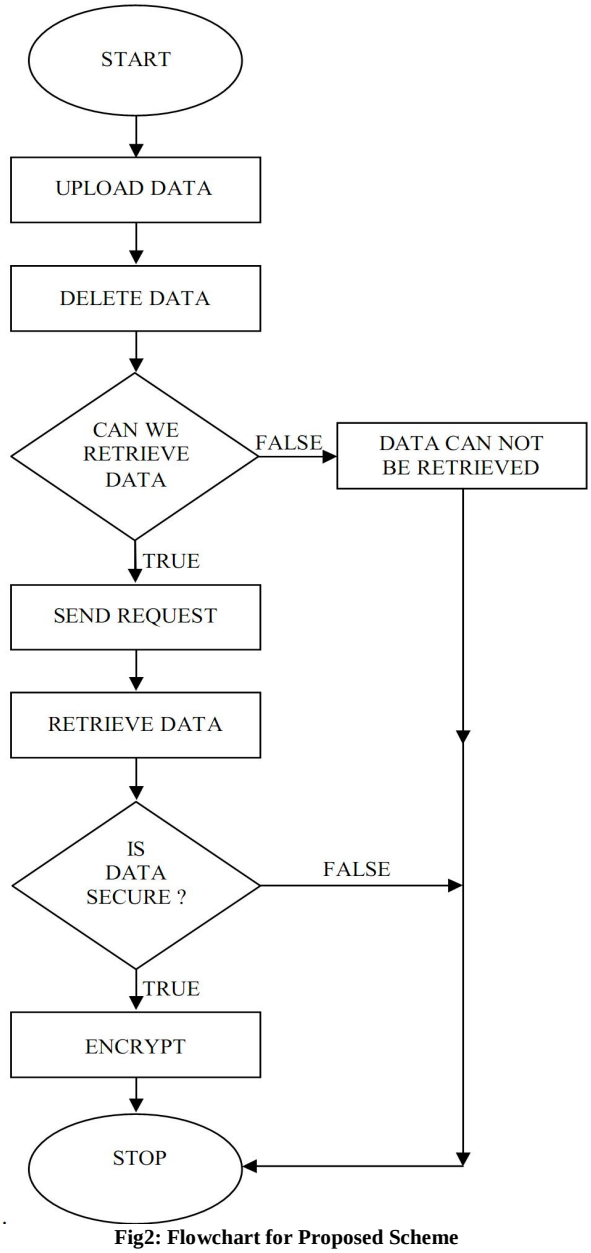

Fig2: Flowchart for Proposed Scheme

Step 17Object = RMcrypto
/* Managing of cryptosystem is done using the above object. */
Step 18Modes = Write
/*After password authentication, we can create the file in different file modes. */
Step 19Object =cs
/* Cryptostream is call by the above object. */
Step 20Object =fsIn
Parameters = inputFile, FileMode.open
/* Input file is call by the above object.*/
Step 21Object =cs
/* Using 'FileStream', we can write in cryptostream
using the above object. */
Step 22 Object = fsIn, cs and fscrypt
/* Closing is done with the above objects respectively. */
Step23 Object= newFile
Parameters = StrPath, FileMode.Create
/* Now, we will create the file using the above object. */
Step 24Object= newFile
/* Now we will write data to the file using the above object. */
Step 25Close the file using object newFile.

The algorithm for restoring deleted file from cloud sever file is as follows:
Step 1 The file is created with the name 'CheckFiles'.
Step 2 Parameter = object sender, EventArgs e
Step 3 Set the directory path after loading the page.
Step 4 Object = gvDetails
/* Details of the file are obtained using the above object . */
Step 5 Object = gvDetails
/* Now, we will bind the data using the above object . */
Step 6 Object = object sender, EventArgs e
/* 'lblRecover' button is created using click event having the above parameters. */
Step7 Sender information is linked through 'LinkButton' using the command argument.
Step8 Source Path and Target Path are set through 'AppDomain'.
Step 9 Use Path class to manipulate file and directory path.
Step 10Through 'input output command', we can copy the file from source to destination and overwrite the destination file if it already exists.
Step 11Parameter = string inputFile, string outputFile
/*To perform decryption, file is created with the name 'DecryptFile' having the above parameters. */
Step 12File is decrypted using the authenticate password.
Step13 Object=fscrypt
Parameter = inputFile, Filemode.Open
/*FileStream is created with the above object . */
Step 14Object = cs, RMcrypto
/* Decryption is done using the above object . */
Step 15Object = RMcrypto
/* Managing of cryptosystem is done using the above object. */
Step 16Object = fsOut
Parameter = outputFile, Filemode.Create
/*Decryption of file stream is done with the above object having the above parameters. */
Step 17Object = fsOut, cs, RMcrypto
/* Closing is done with the above objects respectively. */
Step 18Parameter = object sender, GridViewRowEventArgs event = RowDataBound
/*Data is recovered through 'gvDetails_RowDataBound' using the above parameters. */
Step 19We can recover the deleted data through 'LinkButton'.

IV. RESULT AND SIMULATION

The evaluation of the proposed scheme describe in the previous section is being shown here. The experimental setup consists of static resources and dynamic resources. Static resources consist of local server where applications are hosted and for dynamic server we have assumed a cloud. Here we present a formal analysis of the security of our proposed scheme. Firstly, we will upload a document which will be stored on cloud in encrypted form which is shown in fig 3 and fig 4.

Fig 3: Snapshot for uploading a document

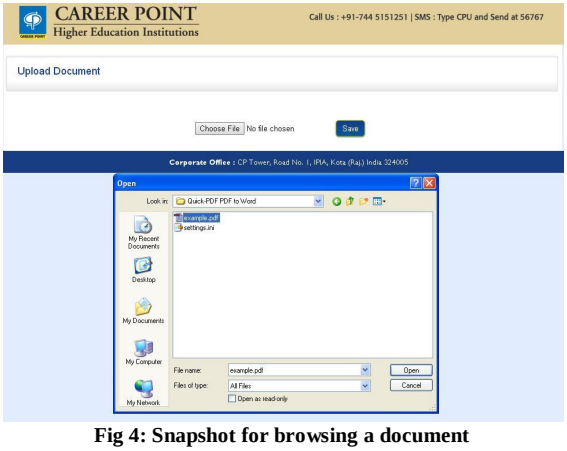

Fig 4: Snapshot for browsing a document

Since data can't be deleted completed, therefore, it is stored on the cloud in encrypted form. In order to recover a data, encrypted data on the cloud will be decrypted and we will recover the desired data which is shown in fig 5.

Fig 5: Snapshot for recovering a document

In the proposed scheme, dot net bench mark is created and the simulation parameters are shown in the table 2 which is shown below.

TABLE 2: PARAMETER TABLE

S. No.	Parameter Name	Value
1	Website Server	1
2	Cloud Server	1
3	User	Multiple

CONCLUSION AND FUTURE WORK

Cloud computing brings many advantages to us and cloud providers enables companies to have access to very powerful resources and solution without any capital expenditure .Here we have discussed about threats found in Cloud computing. Countermeasures for various threats are provided, but, new security techniques are also required. Here, we have focused on the security of SaaS, in the near future, we want security measures for IaaS model including threats such as VM hoping and denial of service.

REFERENCES

[1] Daniele Catteddu and Giles Hogben,"ENISA Cloud Computing: benefits, risks and recommendations for information Security", 2009. Available: http://www.enisa.europa.eu/activities/riskmanagement/

[2] Grobauer B, Walloschek T, Stocker E , "Understanding Cloud Computing vulnerabilities" , IEEE Security Privacy 9(2):50–57,2011

[3] Morsy MA, Grundy J, Müller I, "An analysis of the Cloud Computing Security problem", In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia,2010.

[4] Grobauer B, Walloschek T, Stocker E , "Understanding Cloud Computing vulnerabilities" ,IEEE Security Privacy 9(2):50–57,2011.

[5] Garfinkel T, Rosenblum M, "When virtual is harder than real: Security challenges in virtual machine based computing environments", In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. Volume 10. USENIX Association Berkeley, CA, USA, pp 227–229,2005.

[6] Sniffing /spoofing, available at www.computechdoc.org/ independent/security/terms/attack.html

[7] Reuben JS, "A survey on virtual machine Security. Seminar on Network Security", Technical report, Helsinki University of Technology, October 2007.

[8] Data scavenging, available at flylib.com/books/ en/ 1.564.1.85/ 1/

[9] Michael Miller, "Cloud Computing: web based applications that change the way you work and collaborate online".

[10] Mr. D. Kishore Kumar, Dr.G.Venkatewara Rao, Dr.G.Srinivasa Rao, "Cloud Computing: An Analysis of Its Challenges & Security Issues", IJCSN, oct 2012.

[11] "Security guidance for critical areas of focus in Cloud Computing V3.0.." Cloud Seecurity Alliancce,2011 Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf .

[12] Zissis D, Lekkas D , "Addressing Cloud Computing Security issues", FuturGener Comput Syst 28(3):583–592,2012.

[13] Marinos A, Briscoe G, "Community Cloud Computing", In: 1st International Conference on Cloud Computing (Cloud Com), Beijing, China. Springer-Verlag Berlin, Heidelberg,2009.

[14] Juniper Networks. Inc., "Security Multi-Tenancy and Cloud Computing",2012.

[15] Subashini S, Kavitha V, " A survey on Security issues in service delivery models of Cloud Computing", J Netw Comput Appl 34(1):1–11,2011.

[16] William Stalling, "Cryptography and network security",2013.

[17] Nigel P. Smart and Frederik Vercautern, "Fully homomorphic Encryption with Relatively Small Key and Ciphertext Sizes" International Association for Cryptologic 2010.

[18] SSL available at www.digicent.com/ssl.htm.

[19] Cloud Security Alliance, "SecaaS implementation guidance, category 1: identity and Access management," 2012. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf.

[20] Dynamic credential ,available at infocenter.sybase.com

[21] TCCP, available at www.usenix.org

[22] Berger S, Cáceres R, Goldman K, Pendarakis D, Perez R, Rao JR, Rom E, SailerR, Schildhauer W, Srinivasan D, Tal S, Valdez E "Security for the Cloud infrastructure: trusted virtual data center implementation", IBM J Res Dev 53(4):560–571,2009.

[23] Wang Z, Jiang X "HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity", In: Proceedings of the IEEE symposium on Security and privacy. IEEE Computer Society, Washington, DC, USA, pp 380–395,2010.

[24] Mirage , available at www.openmirage.org

[25] PALM, available at www.webopedia.com

[26] Wang Sumei, "VNSS: A network security sandbox for virtual computing environment", Information Computing and Telecommunications (YC-ICT), 2010 IEEE Youth Conference.

[27] Wu H, Ding Y, Winer C, Yao L ,'"Network Security for virtual machine in Cloud Computing", In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21,2010.

★★★