Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2016, Vol. 8, No. 4

Security Mapping of a Usage Based Cloud System

Kamatchi R.
Amity University, Mumbai
rkamatchiiyer@gmail.com

Kimaya Ambekar
K. J. Somaiya Institute of Management Studies & Research, Mumbai.
kimaya.ambekar@somaiya.edu

Yash Parikh
IndusInd Bank, Mumbai
yash0924@gmail.com

Received: October 31, 2016 Accepted: December 30, 2016 Published: December 31, 2016

DOI: 10.5296/npa.v8i4.10240 URL: http://dx.doi.org/10.5296/npa.v8i4.10240

Abstract

The popularity of cloud computing technology is increasing tremendously. There is no disagreement about the effectiveness of the data storage and the data transition techniques of clouds. Earlier it used distributed computing just for sharing resources. However, with technology advancement, cloud computing has become more and more powerful as well as more adaptive in various business sectors. However, with the increase in number of users, there is also an increase in the security threats affecting the users' privacy, personal data, identity and confidentiality. In this paper, we have aimed at categorizing security and privacy threats based on the kind of usage of cloud. We have also presented an algorithm to find the appropriate solution to address the security and privacy related issues as per the usage category. The case study method is adopted to analyze the pertinence of the algorithm through relevant real time cases. This paper helps in improving security and privacy of cloud technology users without compromising the benefits of data storage.

Keywords: Cloud computing, Security levels, security attacks, solutions

1. Introduction

Cloud computing is a new dimension to the information Technology with extensive benefits. It is a combination of older technologies in new wrapper. It incorporates utility computing, virtualization, web 2.0, Service Oriented Architecture (SOA) and some concepts of distributed computing like grid and cluster computing. Earlier it used distributed computing just for sharing resources. However, with technology advancement, cloud computing has become more and more powerful as well as more adaptive in various business sectors.

Cloud computing can be seen as an elastic, on-demand scalable, pay-as-you-go model. Due to its versatile characteristics, not only big market players but also SMEs also adapting cloud computing.

Depending upon its methods of deployment, cloud computing is divided into four types:

- **Public Cloud:** It is a type of cloud, which is hosted and maintained by cloud service provider (CSP). All users share the infrastructure.
- **Private Cloud:** The services are dedicated for an organization. It can be maintained on site or off site.
- **Hybrid Cloud:** This will be a combination of more than two deployment options. An organization can opt for one service from public and other from private cloud provider
- **Community Cloud:** Organizations who share same goal, mission etc can connect and use cloud services provided by CSP.

Depending upon the types of services it provides, cloud computing majorly divided into following three types:

- **Infrastructure-as-a-service:**

IaaS service providers like, Amazon (EC2), Rackspace provide complete Infrastructure, storage, networks, computational power etc. Majorly, IT administrators, IT managers use this type of service.

- **Platform as a service:**

PaaS providers like Microsoft Azure, EngineYard, and Force.com provide application hosting platforms (E.g. Linux, android), platforms on which applications can be created and database. Users does not own infrastructure but have control over the applications they create. These services are mostly used by developers and researchers.

- **Software as a service:**

SaaS providers like GoogleApps, Salesforce provide applications or software as a service which users can run using browsers. Users do not worry about installation, up-gradation. These services are mainly used by non-technical users and middle level as well as high-level management people.

There are variety of services present in the cloud basket and as a major advantage of cloud, it reduces Capex (capital expenditure) and gives scope to the organization to invest more in OpeX (Operational Expenditure).With all the advantages, the major disadvantage can be seen in security area. Security area shows the major lacuna which needs to be filled using various ways. Not one way can fulfill all the security requirements. A cloud service providers need to use various security measures to create a complete secure experience for the cloud users. The security requirements depend upon various factors. The factors can be seen as types of users, types of services users use, or types of deployment methods CSP uses etc. While creating a complete security policy for a particular individual or an organization, cloud service provider needs to consider all such things. [1]

This paper is organized in seven sections. Current section describes about cloud computing as latest technology. The next section (section 2) talks about types of users in cloud depending upon the need and usage. Section 3 identifies different levels of security for organizations and cloud service providers. This section also maps security levels with types of users. In Section 4, we try to identify different threats and attack on cloud services on the basis of security levels we identified earlier. Section 5 presented an algorithm which will help any type of user to find out the security level he/she may need, threats and/or attacks they may face and possible measures they can take. Section 6 elaborates the algorithm from section 5 using a hypothetical case. In section 7 we conclude and propose some future work.

2. Cloud Users

It is very important to understand the users and usage models. When cloud service providers will have the clear picture of it then only they can create a concrete security plan for organizations. According to the research, there are following types of users who uses cloud services for different reasons [2].

2.1 Naive users:

These users use browsers or applications to access cloud services. Instead of using local applications/ softwares, these users can use them from browsers like Mozilla or Chrome. These types of cloud services reduce the critical installations and update tasks of users. Users should not be worried about the handling and storage of the application. Cloud service providers manage these things. These types of services remove or decrease the dependency on particular operating system. These services will be in the form of web services or application

2.2. Virtualized device users:

These users are more specialized than the naïve users. They use virtualized environment to access different services. Powerful Servers may use different softwares like KVM, VMware vSphere or virtual bridge verde etc to create virtualized environment for users. There servers may have different applications for users. Users just need access through internet to those virtualized machines. E.g., User can have LINUX operating system on his/her system and can access a virtualized desktop on cloud with windows operating system.

2.3. Software developers/ Business developers/researchers:

Software/business developers or researchers may need resources like computational power, storage or different platforms and IDE (Integrated Development Environment) etc. There might be fluctuation in the number of resources needed at a given time. E.g.At the time of compilation, linking or testing an individual may need more resources. On the other hand, there may be a situation where a project may need more people to finish it on time. In such scenarios, organizations may need more certified platforms to work on. Applications like Team foundation server or github can help the organizations to manage coding and deployment of the applications prepared by different developers across. In short, Organization’s needs may be flexible and elastic and those can be fulfilled by cloud services.

2.4. IT System Administrators:

Every organization needs extensive IT support. Bigger organizations have their own datacenter. Smaller organizations cannot afford the data centers. Still they also have their servers and data storage devices. Since computational power and data storage-backup are essentials, every organization has System Administrator to handle the datacenters. These users do not use these services directly but deploy for the organizational employees. Administrators should know the resource requirements and security policies of the organization. These users deploy applications and platforms on the underlined hardware. These users are responsible for the availability, reliability, and scalability of the resources needed by the organization.

3. Security Levels

Cloud computing security has different levels. [3] These levels help organizations and CSPs (Cloud service providers) to implement security measures. These can be divided in following broad categories:

3.1 Physical Level

Any organizations having own data center or CSP having own cloud services, need to have this primitive level security. In this level, securing the campus around the data centers, employing security guards, access regulations, noting down the essential information of the visitors etc can be employed throughout the area. This level is vulnerable for infrastructure damage due to physical/natural disaster, human accidents, and malicious attacks from internal or external personnel.

3.2 Host/Virtual Level

Virtualization is a heart of Cloud computing. CSPs use virtualized environment to provide services to different users. CSPs cannot share the information about virtual images, virtual operating systems they used.

Intruders try to intrude from hypervisor so its security becomes very essential. [4] Hypervisors are always single point of security failure. If one hypervisor is hijacked by attacker then it can damage the whole cloud system. [5]

3.3 Network Level

Networks become essential connectors of cloud computing. Users are connected to the cloud service through networks. The data communication happens via network. That is why it is very necessary to secure the network first. There are varieties of attacks that can be simulated through it. It can ranges from passive to active attacks and can hamper confidentiality, integrity and availability. Cloud service providers should ensure the protocols used are secured and robust. [6] [7]

3.4 Interface Level

Interface for the services offered to the users and the operating system on which the services run should be secured. CSPs these days create services on linux operating system, which is open source and gives more security than other Os [4]. E.g. IBM bluemix is cloud service based on Linux; on the other hand, Microsoft azure is built on windows operating system. [8]

3.5 Operating System Level

Operating system is very important part of the cloud host machine. Apart from bare metal hypervisor, all hypervisors have an operating system. Each virtual machine sits on the operating system that is why operating system security is very important. If operating system is compromised then all virtual machines can be in attack zone. [9] [10] [11]

3.6 Database level

Data becomes very important asset for any organization. Users, which are moving to the cloud services, may need to store the data to the CSP side. It is very essential to understand the importance of the data at rest on CSP’s servers. Most CSPs encrypt data while on transit but only 8.4% CSPs do not encrypt data white at rest. The organizations that offer sensitive data e.g. financial organizations need extra level of security on database. [7] [12] [13] [14]

3.7 Application Level:

The application level of security is the last level of security**.** This will decide who is authorized to access the services and how they will access it. This level of security also ensures attacker should not get control on hardware and applications. This will be assured by CSPs using identity, role, key or claim based access methods. These methods will assure what type of user will see what part of the services. It reduces unintentional as well as intentional data theft and other active or passive attacks on services. [15] [16]

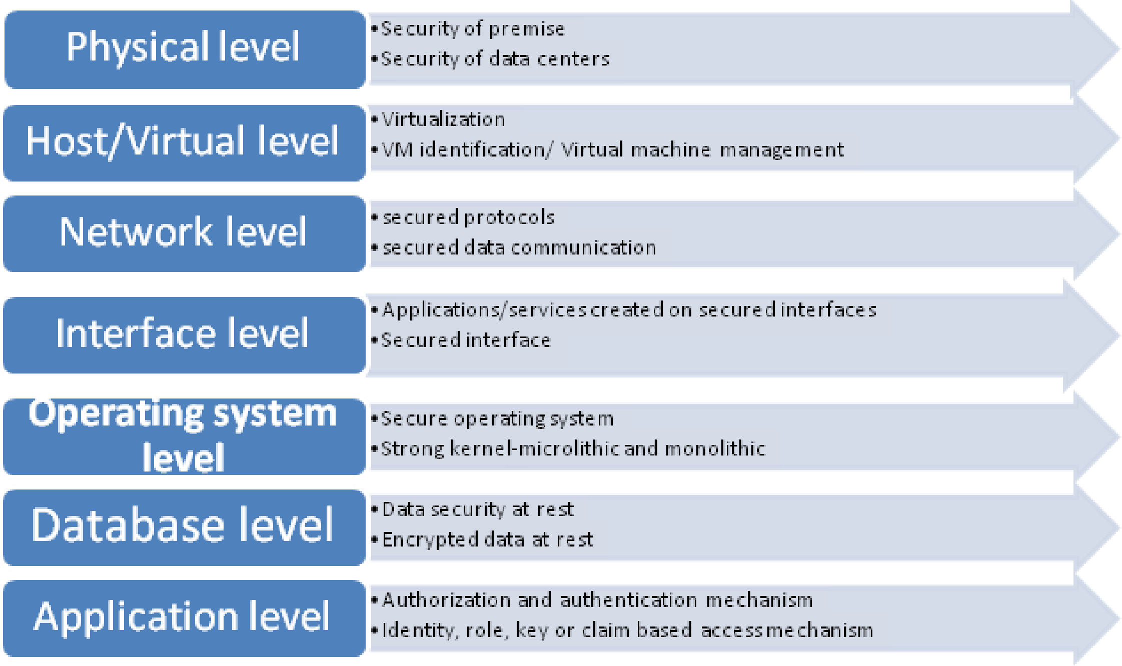
Physical level
•Security of premise
•Security of data centers
Host/Virtual level
•Virtualization
•VM identification/ Virtual machine management
Network level
•secured protocols
•secured data communication
Interface level
•Applications/services created on secured interfaces
•Secured interface
Operating system level
•Secure operating system
•Strong kernel-microlithic and monolithic
Database level
•Data security at rest
•Encrypted data at rest
Application level
•Authorization and authentication mechanism
•Identity, role, key or claim based access mechanism

Figure 1: Security Levels in cloud computing

Table 1: mapping of cloud service users with security levels

Users	Type of Cloud Service used	Security level*						
		Physical Level	**Host/ Virtual Level**	**N/w Level**	**DB level**	**OS Level**	**Interface Level**	**Application Level**
Naïve Users	SaaS						√	√
Virtualized device users	SaaS		√				√	√
Application/ Business developers or researchers	Especially PaaS		√	√	√	√		
IT System Administrators	IaaS	√	√	√				
***Assumption: Basic security is provided for every service in cloud computing Eg: authentication, SSL protocol, VPN etc**								

The above table shows the association between the type of users with the type of services they used and the levels of security they may need

4. Threats and attacks in cloud computing

National Information Assurance Glossary defines threat as any circumstance or event with the potential to adversely impact on IS or any organizational operations (including mission, functions, image, or reputation) through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Attack is a technique used by the attacker to exploit vulnerabilities and create threats to the system. Each security level shows different types of threats and vulnerable for different attacks [17].

Following are the tables, which describe attacks that can be seen under various security levels with the possible solution for each. Table 2 emphasizes physical security attacks, table 3 talks about virtual/host level security attacks; table 4 is for network level attacks, table 5 database level attacks, table 6 about operating system level attacks, table 7 demonstrates interface level attacks and finally table 8 emphasizes on application level attacks and solution.

4.1 Physical Security Level:

Table 2: Physical security attacks and solution

Attacks	Description	Solutions
Stealing data	Insider or outsider can steal the data from the servers due to insufficient security	• Strict security • surveillance cameras • log books which need to be signed before and after visiting the data centers • thorough checking of personnel coming and going • USB slots disabling
Hardware interruption	System hardware is accessed by unauthorized users which may denies the access to legitimate users	
Hardware theft	Due to security, hardware can be stolen	
Hardware modification	Unnecessary hardware modification is done by unauthorized person which may deteriorate the service	
Misuse of infrastructure	Misuse like blackmail or stealing etc can be done by attacker using the existing cloud infrastructure	
Natural disasters	Flood, Electricity failure, lightning etc. may affect and fail the cloud set up	

4.2 Virtual/Host Security Level:

Table 3: Host/virtual level security threats with possible solutions

Attacks	Description	Suggestions
Side channel attack	Attacker places his/her malicious VM on the same physical machine and tries to extract the information as a second phase of attack	• VM isolation, • Encrypted data at rest, • Stop the data leakage
Malware injection attack/Meta-data spoofing attack	Attacker adds an extra service in the existing cloud services pool and steals the data from the authorized. Attacker also install any mischievous software on users device	• When users log in to the CSPs portal, CSP should add the VM image into its image storage system. This can be monitored and integrity is checked periodically.
Zombie attack	Attacker floods users with requests from an innocent host within the network. This may lead to DOS/EDOS attack.	• IDP/IPS • Better authorization and authentication system
Service injection attack	Intruder adds harmful services into the list of cloud provider services that may redirect valid request to invalid services.	• Strong VM isolation and hardening is recommended

VM escape	Attacker runs a malicious script in a VM which destroys the isolation layer between the VMs' and can give access to other VMs as well as to the host OS	• Strong Intrusion Detection System and strong Intrusion Prevention System should be implemented. • Strong VM isolation and hardening needed. • Also powerful firewall can be implemented
Rootkit in hypervisor	Attacker installs a malicious hypervisor that is a new Host os for other guests. This gives freedom to the attacker to run any other code in the environment	
Wrapping attack	Intruder adds malicious code in SOAP (Simple Object Access Protocol) messages in Transport Layer Service (TLS). This messages will then saved to the server which may interrupt server working	• One extra bit-STAMP bit is added in SOAP message header
VM theft	intruder can create or shift the virtual machine that gives the unauthorized control over the virtual machine	• Strong Intrusion Detection System and strong Intrusion Prevention System should be implemented • Strong VM isolation and hardening needed
Hyperjacking	Intruder can introduce a VMM(virtual machine monitor) or a faulty hypervisor which may give the access of all the VM available on the server	

4.3 Network Security Level:

Table 4: Network level security threats with possible solutions

Attacks	**Description**	**Suggestions**
Eavesdropping	Attacker intercepts the network and listens the conversation between the parties which compromises the confidentiality	• Use anti-virus softwares • Implement IPSeC protocol
Replay Attack	Intruder eavesdrop the conversation and may save the data that can be used to create a new connection. This time intruder gets the access of the victim's account.	• Session tokens • timestamps • one time password(OTP) • Two way authentication
In Sybil attack	In this attack, attacker creates multiple fake identities by which they contact genuine users. Then it gives attacker the access to genuine user's account	• Different validation techniques like identity based, role based etc must be implemented
Reused IP address	In cloud computing, IP of a certain service for a user can be reassigned to another user. It will remain in the DNS cache. It can be used by an attacker to get into the system	• ARP addresses should be cleared from the cache regularly

DNS attack	Attacker introduces a wrong DNS address with respect to the IP address in the DNS resolver's cache. This will redirect authorized users to the wrong server.	• DNSsec suite can be used. • Firewalls, routers having ability to perform NAT(Network Address Translation) should be used
BGP prefix hijacking	Border Gateway Protocol contains routing table. Sometimes accidentally or deliberately this table may get compromised and traffic may get redirected to the wrong IP	• MD5/TTL (Time-to-live)protection • Filtering options
Sniffer attack	If the data is not properly encrypted then intruder can read the important information.	• Use ARP(Address resolution Protocol) & RTT(Round Trip Time) to detect the sniffer attack
Port scanning	If any user has specified incoming packets from a source to any particular port, then that port becomes vulnerable to attack	• If port scanning detected then the port associated to it should be stop and blocked immediately
Dos/ DDos	Attack on a particular host or a network from multiple sources multiple places around the world. Attack reduces availability for authorized users.	• IDS/IPS(Intrusion Detection System/ Intrusion Prevention System) • Preventive tools like switches, firewall, routers etc • Strong authentication

4.4 Database Security Level:

Table 5: Database level security threats with possible solutions

Attacks	**Description**	**Suggestions**
Data loss and leakage	Due to the shared nature of the cloud, this threat becomes more susceptible. In this unauthorized updation, deletion, removal or extraction of data may happen	• Data encryption at rest • Authentication and authorization • backup and retention policies • Secure APIs and Data integrity checks should be implemented
Access data and control	Due to lack of access control mechanism, confidential information can be seen or used by authorized users	• Access control mechanism can be implemented, • Key based access, various encryption techniques

Data segregation	Multi-tenant architecture helps many users to have their data on the cloud simultaneously. If proper separation does not implemented then the data can be seen by unauthorized user.	• techniques like data validation for insecure storage, • SQL injection Aws etc
Data stealing	User's username and password is stolen and the data is stolen by the attacker	• CSPs can send an email to the users for every session about the time and amount for the session.
Data Location	The location of data storage is not known to the customer. The data can be kept with other customers. Or the location may be not proper according to the company/government policies	• Read and understand the SLA document carefully before proceeding

4.5 Operating System Security Level:

Table 6: Operating system level security threats with possible solutions

Attacks	**Description**	**Suggestions**
Direct access attacks	Attacker may compromise the security by changing parts in OS. By doing this, attacker can modify the OS also can boot another OS or any other malicious application	Trusted platform modules, Disk encryption
Buffer overflow	Attacker control or crash the Operating system by overflowing the buffer. In this data also can be overwritten from the adjacent data buffer.	Patches and upgrades from a valid vendors should be implemented to avoid these attacks
Unpatched operating systems	Operating systems frequently have patches and upgrades for existing vulnerabilities. If the host operating system is not updated then the attacker may exploit the OS	
Exploit Attack	Attacker learns from reconnaissance attack about operating system running on host/guest. After knowing which, attacker may exploit vulnerabilities of OS	Use of OS which uses heuristic termination analysis as a part of it

4.6 Interface Security Level:

Table 7: Interface level security threats with possible solutions

Attacks	**Description**	**Suggestions**
Code injection attack	Malicious code is incorporated into the application's interface. Which gives attacker either the authentication information or privileges to exploit the services more	Use of good encryption techniques
browser hacking	Malicious code is added into the user browsers through cookies. These infected browsers can help intruder to know the authentication details	Use of antivirus applications Don't save cookies

4.7 Application Security Level:

Table 8: Application level security threats with possible solutions

Attacks	**Description**	**Suggestion**
SQL injection attack	Attacker inserts a malicious code into SQL standard queries that gives him access to the database.	A strong user input detection and sanitization systems should be developed and implemented in the cloud environment
cross -site scripting	Intruder adds a code/script into the web page which may be stored permanently or reflected just for the time on the web page	Various technologies like Web Application Vulnerability Detection Technology, Content Filtering, Content Based Data Leakage Prevention Technology etc are available to detect and mitigate the attack
EDos(Economic Denial of Sustainability)	It is an attack on Pay-as-you-go model. Services are used by attacker so much that it obstruct economic drivers of cloud computing	Applications like EDoS-Shield can help in preventing EDOS attacks. It uses cloud verifier node and virtual firewall which filters the requests
Cookie poisoning	Intruder can change the content of the cookie	Cookie saving should be disabled. Cookie cleanup is necessary
Backdoor and debug options	website debugging options if left by the developer then attacker can enter into the website easily and modify the content	At the time of website publishing, debug option should be disabled
Hidden field manipulation	Hidden fields are used by the developers to maintain the state. If it gets noticed then attacker can use to enter in the service	Use as less as possible of hidden fields and also query strings

Man in the middle attack	Intruder sits in between two or more people's communication. Intruder eavesdrop the conversation and also can provide false information to other party	Plenty of tools like Airjack, Cain, Dsniff etc can be used to prevent this attack
DOS/ DDOS	Server becomes unavailable because of flood of requests from unauthorized user/s. The attackers may be placed from different parts of world which contributes in DDOS attack	IDS/IPS(Intrusion Detection System/ Intrusion Prevention System),Preventive tools like switches, firewall, routers etc

5. Algorithm

This paper provides an algorithm to understand what type of security measures an individual should take to have a secure cloud services experience; depending upon the type of user he/she is.

Step 1: Choose the User type from the 4 users type types mentioned earlier U_i ={1…4}

Step 2: Choose the security levels needed for your user type. Sec_i = {1….7}

Step 3: Prioritize the levels according to your need

Step 4: Select the types of attacks according to the security levels needed. Each type of security levels has different possible attacks and their possible solutions

Step 5: Implement the security solutions from the given list or select the CSP after evaluating the effectiveness of their services on the previous solutions

The flowchart for the given algorithm can be given in figure 2 below.

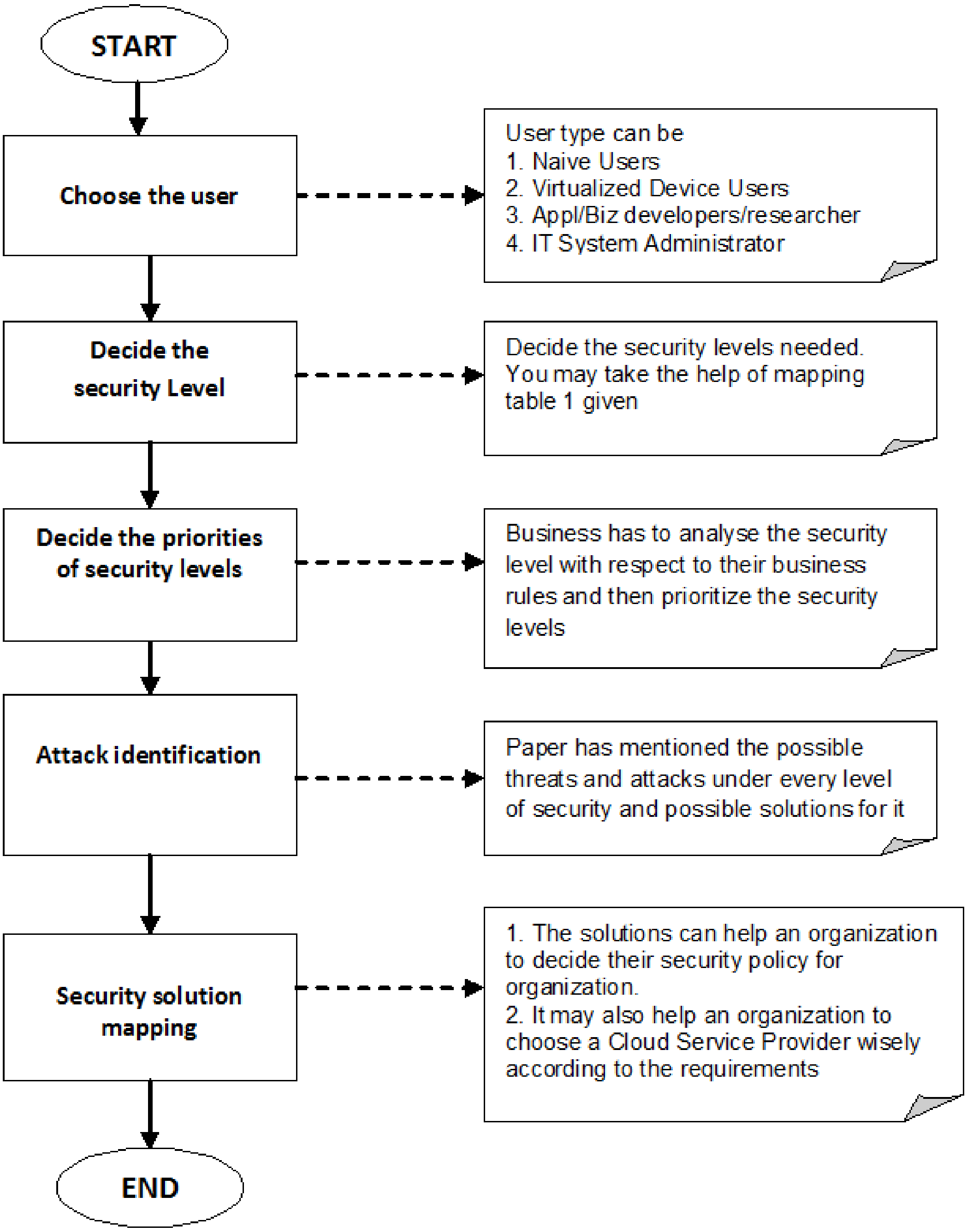
START
Choose the user
User type can be
1. Naive Users
2. Virtualized Device Users
3. Appl/Biz developers/researcher
4. IT System Administrator
Decide the security Level
Decide the security levels needed. You may take the help of mapping table 1 given
Decide the priorities of security levels
Business has to analyse the security level with respect to their business rules and then prioritize the security levels
Attack identification
Paper has mentioned the possible threats and attacks under every level of security and possible solutions for it
Security solution mapping
1. The solutions can help an organization to decide their security policy for organization.
2. It may also help an organization to choose a Cloud Service Provider wisely according to the requirements
END

Figure 2: Detailed Flowchart for the Algorithm

Explanation:

Choose the user

The user will be selected based on the usage level. The different levels of users are defined based on their access mechanism which has to be specified as the first level of this flow

Decide the security level

With the user token, the level of security should be specified. The level of security varies with the services they want to use. These levels will show different levels of security and privacy concerns and needs.

Decide the priorities of security levels

The decision would be validated based on the business rules. This step enables the process of security levels definition more simple and realistic

Attack identification

Every security level engrossed with various possible threats and attacks. The best possible attacks are to be identified and aligned based on the priorities. The top priority attacks should be dealt with immediate effects.

Security solution mapping

As various security solutions are available in today's computer world, the solutions are to be mapped with the requirements and best possible results. The ideal solutions with multiple benefits to be identified and implemented.

6. Case

Mr. Kumar is a middle level manager in the sales and purchase department of garment industry, which is medium level Industry. The organization uses in-house CRM application. Now organization wants to move on cloud where they will be using CRM on cloud and employees will access it through the internet. In order to implement this, they will now have to evaluate the level of security CSPs can provide.

Solution:

S1: User level here is virtualized user (SaaS) because there will be plenty of employees from the same organization will be using the same CRM application on the cloud

S2: According to Table 1, for virtualized users (SaaS), virtual/host level, Interface level and application level security is needed.

S3: Organization may prioritize it as Application level as first, then virtual/host level and then interface level.

S4: According to the attacks and possible solutions following care should be taken by CSP and organization

- Strong VM isolation, VM hardening and appropriate IDS/IPS system should be implemented.
- Data at rest should be encrypted and data leakages should be taken care of.
- Strong authentication, input detection mechanisms should be implemented. Tools that can prevent DOS/DDOS attack can be used. Lessen the use of query strings and hidden fields. Strong content filtering should be used.

S5: Above-mentioned measures should be checked before moving on cloud services. SLA should take care of all the above suggestions. These things should be taken into consideration when a strategic team will evaluate a CSP for adopting cloud services.

7. Conclusion

This study has been performed with the limited samples of four major usage categories with seven different security levels. As the cloud computing technology is cropping up rapidly, this study can be further extended by including more and more subcategories. This paper relates the different threats with the major security issues classification, which can be extended further. The effectiveness of the stated algorithm has been verified using a case analysis method. The analysis report indicates the effective functioning of the proposed algorithm. As a whole, this study provides a successful modus operandi towards a smooth ride in a cloud environment.

8. Reference

[1] Kimaya Ambekar, Kamatchi R., “Enhanced User Authentication Model in Cloud Computing Security”, Intelligent Systems Technologies and Applications 2016, Advances in Intelligent Systems and Computing 530, http://dx.doi.org/10.1007/978-3-319-47952-1_26, Springer International Publishing AG. 2016

[2] Bob Sutor, “Who is the user for cloud computing?”, http://www.sutor.com/newsite/blog-open/?p=4548, accessed on 10/10/2016.

[3] Harpreet Saini, Amandeep Saini, “Security Mechanisms at different Levels in Cloud Infrastructure”, International Journal of Computer Applications. Volume 108 – No. 2, December 2014. http://dx.doi.org/10.5120/18880-0153

[4] Dimitrios Zissis , Dimitrios Lekkas, “Addressing cloud computing security issues”, Future Generation Computer Systems. Vol. 28, Issue 3, March 2012, Pages 583–592 http://dx.doi.org/10.1016/j.future.2010.12.006

[5] Vahid Ashktorab, Seyed Reza Taghizadeh, “Security Threats and Countermeasures in Cloud Computing”, International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 1, Issue 2, October 2012,

[6] R. Charanya, M.Aramudhan, K. Mohan, S. Nithya, “Levels of Security Issues in Cloud Computing”, International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013

[7] Katerina Lourida1, Antonis Mouhtaropoulos2, Alex Vakaloudis3, “Assessing Database and Network Threats in Traditional and Cloud Computing”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(3): 1-17, 2013

[8] Aarti Singh, Manisha Malhotra, “Security Concerns at Various Levels of Cloud Computing Paradigm: A Review”, International Journal of Computer Networks and Applications. Vol. 2, Issue 2, March – April (2015).

[9] Computer security, https://en.wikipedia.org/wiki/Computer_security, accessed on 22/10/2016 at 1:50 pm

[10] Margaret Rouse, “Buffer overflow”,

http://searchsecurity.techtarget.com/definition/buffer-overflow, Accessed on 22/10/2016.

[11] Bogdan Popa, "Unpatched Operating Systems Could Literally Allow Hackers to Kill Patients in Hospitals", http://news.softpedia.com/news/Unpatched-Operating-Systems-Could-Literally-Allow-Hackers-to-Kill-Patients-in-Hospitals-448595.shtml, accessed on 23/10/2016 at 5:00 pm

[12] Kashif Munir and Sellapan Palaniappan, "Security Threats/Attacks Present in Cloud Environment", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012.

[13] Kashif Munir and Prof Dr. Sellapan Palaniappan, "secure cloud architecture", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013

[14] Jaydip Sen, "Security and Privacy Issues in Cloud Computing", Chapter 1. Architectures and Protocols for Secure Information Technology Infrastructures. IGI Global. Pp. 1-45. DOI: 10.4018/978-1-4666-4514-1.ch001

[15] Ankur Pandey,Kirtee Shevade, Roopali Soni , "Application Level Security in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5369-5373

[16] Tauseef Ahmad, Mohammad Amanul Haque, Khaled Al-Nafjan, Asrar Ahmad Ansari, "Development of Cloud Computing and Security Issues", Information and Knowledge Management. Vol.3, No.1, 2013

[17] R kamatchi, Kimaya Ambekar, "Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models", Indian Journal of Science and Technology**,** *Vol 9(21)*, http://dx.doi.org/*10.17485/ijst/2016/v9i21/95282*, *June 2016*

Copyright Disclaimer