International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 5, October 2018, pp. 3129~3139
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp3129-3139

Review on Security Aspects for Cloud Architecture

Shaz Alam, Mohd Muqeem, Suhel Ahmad Khan
Department of Computer Application, Integral University Integral University, India

Article Info

Article history:

Received Jun 10, 2017
Revised Feb 13, 2018
Accepted Aug 27, 2018

Keyword:

Cloud computing
Security in cloud
SPI model

ABSTRACT

Cloud computing is one of the fastest growing and popular technology in the field of computing. As the concept of cloud computing was introduced in 2006. Since then large number of IT industries join the queue to develop many cloud services and put sensitive information over cloud. In fact cloud computing is no doubt the great innovation in the field of computing but at the same time also poses many challenges. Since a large number of organizations migrate their business to cloud and hence it appears as an attractive target for the malicious attack. The purpose of the paper is to review the available literature for security concerns and highlight a relationship between vulnerabilities, attacks and threats in SaaS model. A mapping is being presented to highlight the impact of vulnerabilities and attacks.

Corresponding Author:

Shaz Alam,
Department of Computer Application,
Integral University,
Kursi Road, Lucknow, India.
Email: shaz.alam62@gmail.com

1. INTRODUCTION

Cloud computing emerges as the innovation which reduces the management effort for organization and allows them to focus towards their core functionalities. As per the study of Gartner, cloud computing is among the top ten innovations in the field of computing [1]. Cloud computing provides the computing services, information and memory space at a very reasonable cost. This innovation of computing has many advantages such as business innovation, economy of scale, low administrative overhead, low operation and maintenance cost, high quality services etc. over traditional owned private data centers. Thus Cloud computing appear to be one of the best option for a large number of IT organizations. As per one survey 91% organization in Europe and US accept the fact that cost effectiveness is the main reason to migrate the business to cloud [2]. But it is a proven fact that every coin has two faces i.e. it also has challenges. Generalization of cloud computing make more enterprises, person to put a large amount of sensitive information over cloud. Thus the impact of security issues will be large [3, 4]. A survey regarding cloud services made by IDC highlights the fact that the security is one of the biggest threats in the adoption of Cloud as shown in the Figure 1 [5].

Few well known security incidences occurred in past were as in 2009, the PayPal a payment tool encountered a network broken accident as a consequence of which millions of machines could not sold products for an hour on a global scale [6]. In 2011, the packet switched network of Sony was breached by the hacker which resulted in compromise of personal information of 70 million users [7]. In 2013, the window Azure cloud encountered a global failure caused by the exchange of deployment by virtue of manual operation [8]. All these above past incidences are just because of improper assessment of threats vulnerability and their impact over the system.

Majority of above mentioned incidents were at application level. SaaS model is more risk prone as compare to PaaS and IaaS due to the existence of inherited risk of these models. This may act as driving

force to understand the challenges in SaaS model. Our focus is to study the security risk at different level such as application, transmission and storage. The purpose of the review is to identify different type of existing vulnerabilities exploited by malicious attacker to analyses the impact over the system. In order to understand the topic, research paper is break up into five sections. Section 2 discuss about cloud architecture especially for SaaS model, section 3 discuss about security in cloud architecture. Section 4 give brief literature review, section 5 proposed a mapping between vulnerability, attacks and threats and final section 6 consists of purpose and conclusion about the research.

Figure 1. Impact of security aspect for cloud

2. CLOUD ARCHITECTURE

Cloud Architecture consist of components loosely coupled to each other. These components are broadly categorized in two major components Front End and Back End connected via internet. Front End refers to client part (e.g. web browser, mobile app etc.) and Back End refers to cloud itself. Cloud Provider usually provides three basis levels of services such as IaaS, PaaS and SaaS [9].As per Cloud Security Alliance (CSA) stack model; SaaS inherit all the hidden challenges of PaaS as well as IaaS [10]. Cloud Architecture Skelton for SaaS provider is illustrated as in Figure 2.

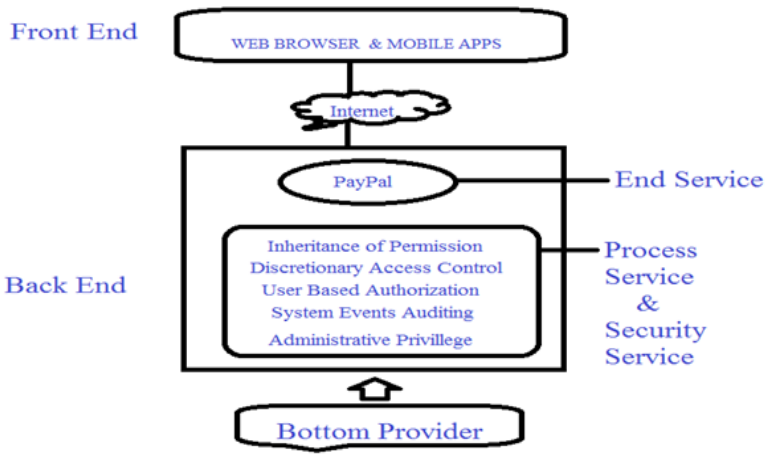

Figure 2. Cloud architecture

Figure 2 represent that SaaS provider consist of two main components one is enterprise service and second one is supportive service. Enterprise services are those ready services that directly serve the clients while supportive are those one who plays a significant role in providing security and maintains to end services. Supportive services includes inheritance of Permission, discretionary access control, user based

authorization, auditing of system events and administrative privilege. Inheritance of permission means that when user creates group then it inherits all the permission rights of its parent group. Discretionary access control reveals the decision of resource owner how it can be shared. It is a type of access control defined by Trusted Computer System Evaluation Criteria. It is helpful to restrict the access to object based on identity, subject and group. User based access control is depend upon role based access control model. This model assigned the roles to user and based on roles access privilege to users is assigned. Auditing of system event is one of the most important steps to ensure the reliability and performance. Administrative Privilege is again related to right to administrative access for protected resources. In the end these SaaS service provider may be supported via bottom providers which also bring many hidden challenges.

3. SECURITY IN CLOUD ARCHITECTURE

In Cloud Architecture, there are two main actors involved in functioning of cloud. They are cloud provider and cloud users. Thus it is required to define the boundaries of responsibilities for security in cloud provider and user. Cloud Security Alliance (CSA) stack model defines the boundaries of responsibilities between provider and user for specific service model [10]. Cloud provider has the maximum responsibilities for SaaS while least for IaaS. It defined security level up to which cloud provider is responsible to manage the concerns.

From all the above description it was cleared that both the actors are responsible to manage and control various security issues. Although the security boundaries are defined still cloud security is one of the nightmares to handle. Occurrence of all the past security incidences was due to existence of different vulnerabilities in cloud system. These incidences may be easily avoidable with the help of an effective approach to identify the vulnerabilities and assess their impact during vulnerability life cycle. This information may be stored and utilize for timely generation of solution patches or to pre inform the cloud user to take some precaution to avoid the exploitation. In the era of cloud security solution, early detection of vulnerabilities and threats is one of the most demanding research topics for current researcher. Currently huge numbers of researches are going on for this topic. But since cloud computing comprises varieties of assets vulnerable to different threat. Hence require serious attention from current researcher of cloud security.

4. LITERATURE REVIEW

This review section contains the views of different authors in existing security issues in cloud architecture: In 2009 Kandukuri, Paturi and Rakshit discussed to include more security management commitment in documentation of Service Level Agreement (SLA).The purpose of this document is to identify & define customer need, provide a framework for better understanding, simplify complex issues, reduce the conflicts, encourage dialog in disputes, and avoid unrealistic expectation. This document comprises of service definition, performance management, problem management, customer duties & responsibilities, warranties & remedies, security, disaster recovery & business continuity and termination polices. This paper highlighted the past SLA issues regarding standard waivers scheme that may not satisfy the customer for loses. Thus it is necessary to issues the waiver as per the business loss and also include various security commitment from cloud provider such as privilege user access, regulatory compliance, data location, data segregation, investigate support, recovery and long term viabilities. It may be viewed as one of the important step to increase the trust of user over cloud provider [11].

In 2010 Cusumano conducted research to highlight threats affect security requirement such as confidentially, integrity and availability known as CIA parameter. During this research, security threats are classified as account control, malicious internal staff, multi-tenant problem, and data control and safety management. Account control is a problem related to service and identity hijacking. Malicious internal staff is one the biggest problem due to existing culprit within the system having access to valuable and sensitive resource. This culprit or malicious staff may not be easily detectable via Intrusion Detection System (IDS) or firewall. Multi-tenant problem are the problems related to effectiveness or robustness of methodologies used these days for isolation purpose during sharing. Data control are problem related data privacy or loss. Safety management is about the effectiveness of prevention mechanism [12]. In same year, Dimitrios Zissis &Lekkas also highlighted same sort of issues such as account control, data control, multi tenancy issues, malicious internal staff and management console as discussed by Cusumano with one more fold towards the suggestion of its solution. Author proposed a solution using the concept Single Sign on (SSO), LDAP to ensure the effective authentication, integrity, confidentially needed for data and its communication [13].In same year, Prasad & Ben proposed a quantitative risk assessment and impact analysis framework. This framework defined risk as a combination of probability of occurrence of security threats and its severe impact

over cloud. This may be viewed as a road map to assess the robustness of different vendors and their approach [14].

In 2011 Feng compared security aspect and their impact over the cloud. In this research, it was concluded that security and privacy of data is among the biggest issues to tackle. Feng also pointed out the absence of effective security rank evaluation and verification system. It was noticed that majority of current on-going research focused on identification threats and suggesting their counter measure techniques without making any rank wise severity comment for a particular threats over the cloud architecture [15].In same year, Subashini & Kavita discussed internal security aspect related to web browser and web service interface API for accessing different services. This paper highlighted the presence of weak authentication, authorization mechanism, week data isolation, segregation and also discussed the multi tenancy problem which makes a significant impact on three very important security parameters confidentially, integrity and availability [16].

In 2012, Joshi and Vijayan carried out their research for zombie attack prevention. In this paper, Cloud Trace Back (CTB) model was suggested as a prevention technique. This model based on deterministic packet marking algorithm. It uses cloud protector consist of virtual firewall to verify the request authenticity of genuine user with help of white and black IP address list [17]. In same year Duan, Chen, Sanchez, Dong also carried out their research in field of zombie attack. This paper introduced a SPOT approach to detect the compromise virtual machine by monitoring outgoing message. It is based on a powerful statistic tool Sequential Probability Ratio Test (SPRT). This SPOT approach depend upon two important terminologies count threshold and percentage threshold to detect the malicious spam message from internal machine [18].

In 2013, Keiko, David, Eduardo conducted their research on threats including account control, malicious internal staff, multi-tenant problem, data control and safety management. The purpose was to highlight lacking in existing system. In the end counter measures are also discussed to reduce or overcome the effect of these threats [19].In same year, Chirag, Dhiren, Bhavesh, Avi, Muttukrishnan took one further step in analysing vulnerabilities, attacks and their corresponding threats. The purpose was to generate a linking between the vulnerabilities, attacks and threats [20]. In same year Jyoti, Ritu, Neha, Monika carried out their research on phishing attack. This paper thrown light on various ways means to plan a phishing attack such as sending bulk mails or by creating a web page similar to well-known websites etc. In the end introduced anti- phishing techniques such as server based technique with help of brand monitoring, behaviour detection, security incidences& client based technique including email analysis, black list, similarity of layout etc. [21].

In 2015, Torkura, Cheng, Meinel conducted their research in development proactive vulnerability assessment framework. Various scanners are deployed for early detection of these flaws in cloud architecture. In this paper, a quantitative risk assessment was conducted over open stack vulnerability life cycle and noticed different risk level due to prolonged patch release and inclusion duration. These risk level are black risk, grey risk and white risk. Existing scanners are working to mitigate white risk only with the help of open source vulnerability database (OSVDB) and National vulnerability database (NVD). This paper proposed a proactive framework for vulnerability assessment to mitigate the risk levels in grey and black level with help of including more dynamic sources such as Bug Tracking System (BTS), malicious signature repository and exploited database (EDB) [22].

In same year Masky, Young, Choe proposed Operationally Critical Threats Asset Vulnerability Evaluation (OCTAVE) as a novel risk identification framework for security issues. It was noticed that occurrence of various threats is due to improper identification and impact assessment of risk over cloud. This proposed framework performed the working in four phases consist of eight steps. First phase is about to develop a risk measurement criteria around qualitative parameter such as Reputation / Confidence, Financial Requirement, Productivity, Safety and Health, Fine and legal penalties with priority wise ranking. In phase 2 all the information asset that are identified to be critical are profiled. This profiling includes the identification of security requirement of information asset and also identifies the container where it is stored, transported and processed. Phase 3 is about to identify the threats to information asset. In final phase identify the risk to the information asset. This risk may be viewed as combination of threats with their adverse impact over the system. Finally include the analysis and suggesting mitigation approach [23].

In 2016, Dang, Lei, Zhang, Shuai and Zhuang carried out their research on various security aspects in software as a service model. Depending upon the analysis, it was divided into three major components such as application, transmission and storage. This paper proposed two very important model Analytical model and Relational model. The purpose of these models was to enrich knowledge bank for well-known problem occurred in past and finally create a linking with its solution using relational model [24].In same year, Rakshita carried out their research in zombie attack detection and prevention. In this a framework was proposed to detect and prevent from Zombie attack. Framework works in two phases, phase consist of a light weight network intrusion detector was placed over cloud server to scan vulnerabilities, and attack to establish

a scenario attack graph and this graph was utilized to decide that whether network should be put under inspection or not. If yes then in phase 2 reconfiguration of virtual network have taken place [25].

4.1. Review Observation

The said review stated security revolves around three important terms vulnerability, attack and threats. Volume of ongoing research is to fetch out attacks and their associated threats. But very limited number of studies focused to get the answers for what is the reason of these attacks. Early detection of vulnerabilities is one of the alternatives to avoid these attacks and threats. This also brings a great emphasis to take a strong correlation between different security anomalies identification and managing relation to security. The intended threats, vulnerabilities and attacks took the functionalities of SaaS services under malicious phase and get harm to services and software. Table 1 shown literature review summary.

Table 1. Literature Review Summary

S.No	Author/Reference	Year	Research Topic	Finding	Limitation
1	Kandukuri [11]	2009	Cloud security issues	Define ways to include more commitment in SLA from cloud provider.	Not discuss about security issues from user end.
	Cusumano [12]	2010	Cloud computing and SaaS as new computing platform	Classification of threat	Not discuss about counter measure.
3	Dimitrios [13]	2010	Addressing cloud computing security issues	Classification of threats and suggested their counter measures.	Not discuss about the authenticity of counter measure.
4	Prasad [14]	2010	QUIRIC: A Quantitative impact and risk assessment framework for cloud security	Quantitative Risk Assessment Framework.	Question on Authenticity and Broad acceptance of framework.
5	Feng [15]	2011	Study on cloud computing security	Comparison of threats and pointed towards the absence of rank evaluation system.	Require a discussion how to develop such system.
6	Subashini [16]	2011	A survey on security problems in service delivery models of cloud computing	Classification of threats at client side (internal threats related to browser)	Require more light on existing client architecture to avoid these threats.
7	Joshi [17]	2012	Securing cloud computing environment against DDoS attacks.	Proposed a Cloud Trace Model for Zombie Attack Prevention.	Question on Authenticity and Broad acceptance of model.
8	Duan [18]	2013	Detecting spam zombies by monitoring outgoing messages	Proposed a SPOT approach for Zombie Attack Detection	Question on authenticity and Broad acceptance of model.
9	Keiko [19]	2013	An analysis of security issues for cloud computing	Discussed about vulnerability in existing system for early removal of threats.	Require more extension about vulnerability and its linking with threats.
10	Chirag [20]	2013	A survey on security issues and solution at different layers of cloud computing	Proposed a linking between vulnerability and threats.	Require suggestion to overcome these vulnerabilities.
11	Jyoti [21]	2013	Phishing & anti phishing technique : case study	Highlighted the ways to plan phishing attack and proposed anti-phishing technique.	Question on authenticity and Broad acceptance of technique.
12	Torkura [22]	2015	A proposed framework for proactive vulnerability assessment in cloud	Vulnerability Assessment Framework	Question on authenticity and Broad acceptance.
13	Masky [23]	2015	A novel risk identification framework for cloud computing security	Proposed an OCTAVE (Operationally Critically Threats Assets Vulnerability Evaluation) approach	Question on authenticity and Broad acceptance and limited to storage asset only.
14	Dang [24]	2016	Security analysis model, system architecture and relational model of cloud services	Proposed two models relational model and analytical model to enrich security knowledge bank.	Question on authenticity and Broad acceptance

5. ESTABLISH A MAPPING BETWEEN VULNERABILITIES, ATTACKS AND THREATS

The purpose of this section is to list out vulnerabilities, attacks and corresponding threats. Main focus of the listing is to fetch out a concrete mapping between vulnerability, attacks and threats. With the help of proposed mapping, main aim is to highlight the impact of vulnerabilities & attacks in different area of major concern.

5.1. Classification of Vulnerabilities

Vulnerability is referred to be as flaws in existing system. These flaws may be exploiting by the different malicious attacker to harm the system. Since this model was recently introduced and new to computing world has many loop holes are as follows:

5.1.1. Employee and Cloud User Unawareness

Lack of awareness of employee and its users about system in IT industry continues to be nightmare for cloud computing. This loop holes can be exploit by attackers to plan zombie attack [18, 25] and phishing attack [21]. Reasons for the existence of these vulnerabilities are poor hiring strategy& background check up, lack of employee screening & security education impartment [10, 33].

5.1.2. Easy and Un-authorised Access

Management interface are easily accessible over internet. Although the cryptography was used to prevent from unauthorized access but advancement in crypt analysis makes a strong encryption to weak encryption e.g. a cryptographic hole discovered in Amazon EC2 management interface by performing signature wrapping and cross site scripting (XSS) attacks, whereby interfaces used to manage cloud resource are hijacked. It allows creating, modifying and deleting machines images, change administrative password and setting [34].This may cause zombie attack [18, 25], phishing attack [21] and service injection attack [26 to 28] etc.

5.1.3. Lacking in Concept of Virtualization

Virtualization is the base to share single resource among multiple tenants. In cloud architecture virtual machines comprises of application software and guest operating system running controlled via hypervisor in host operating system. Many times it was noticed that malicious internal staff got access over host operating system to compromise hypervisor to gain access of guest machine. For examples, a malformed code in Microsoft's Hyper-V run by an authenticated user (internal employee) in one of the VM caused a Denial of Service, by compromising the Hypervisor, an attacker can gain control over VMs BLUEPILL [29], Sub Virt [30], and DKSM [31]**.**

5.1.4. Lacking in Internet Protocol

Flaw in authentication mechanism, validation techniques, week mutual authentication mechanism utilized by attackers to plan ARP spoofing, DNS poisoning and Man-in-the-middle-attack [20].

5.1.5. Web Browsers and In-Secure API

Cloud services are accessible with help of web browser and API. But infection in web browser due to unwanted visits to malicious website and presence of insecure API due to weak access credential, poor authorization and input validation techniques [19] are vulnerable to malicious activities such Phishing attack [21], and Service Injection attack [26-28].

5.1.6. Data Storage Related Vulnerabilities

Data of multiple tenants are stored at same location. Such storage may ask questions on robustness of segregation and isolation mechanism for data of multiple tenants which was stored under different jurisdictions or places. It also caused the problem of incomplete or insecure data deletion**,** transparency [19], and meta-data spoofing attack [20].

5.2. Classification of Attacks

Attack may be defined as way of exploiting vulnerabilities to harm the system. Different types of attack are listed as:

5.2.1. Zombie Attack

An attacker compromise host to plan a Zombie attack [20]. These hosts are used by hacker to send large number of request for a virtual machine. This interrupts the expected behavior of cloud computing affecting their availability. It overloaded the cloud to serve large number of request, and then exhausted to cause Denial of Service (DoS) or Distributed Denial of Services (DDoS) [17]. This may be prevented via a better authentication, authorization and IDS/IPS to avoid the hacking of their system to avoid Zombie attack e.g. A denial of service attack against BitBucket.org, a code hosting site, caused an outage of over 19 hour of downtime during an apparent denial of service attack on the Amazon Cloud Infrastructure [32].

5.2.2. Service Injection Attack

Due to the facility of free to use instance of requested services and easily accessible management interface allows an adversary to plan or inject a malicious service or create a new virtual machine [20]. If attacker succeeds in doing so, then the valid request can be redirected to malicious services automatically. This would results in threats like customer data manipulation, account or service hijacking. This may be avoided by strong isolation or identification mechanism for virtual machine, or by implementing service integrity.

5.2.3. Attack on Virtualization

VM Escape. A malicious program running in virtual machine allows the attacker to directly interact with Hypervisor. This allows an attacker to gain access over host OS and then compromising guest OS controlled by host OS [20].

5.2.4. Man-in-the-middle Attack

Man-in-the-middle attack follows chess analogy of either win or draw a game. It makes an independent connection with the victims and relay or alter the message between them. It helps an attacker gain access over sensitive information or may manipulate the customer data. It is due to flaws in internet protocol, weak password to gain access over a wireless network and weak mutual understandable authentication mechanism. [20].

5.2.5. ARP Spoofing

Attacker sends a falsified ARP message to connect IP address with a malicious host. This is because ARP does not require proof of origin for source. This flaw may be utilized by the attacker to plan ARP spoofing attack to redirect a customer to a malicious host [20].

5.2.6. DNS Poisoning

DNS servers provide a mapping between the domain names to specific IP address with the help its domain resolver cache. If cache consists of a corrupt domain name mapping would result in landing the customer to a malicious website. This is due to flaws in DNS software and source validation mechanism [20]

5.2.7. Meta Data Spoofing Attack

Presence of weak authentication, authorization mechanism, and malicious internal staff with outdated encryption technique allows an attacker to change or modify the information about the services stored in web service description language (WSDL) file at delivery time. It helps the attacker to gain access over various important application or sensitive information [20].

5.2.8. Phishing Attack

An attacker may use the web services to manipulate the link and redirect the customer to false website to steal or fetch the sensitive information. There are number of way means used these days to plan a Phishing attack. This results in account or service hijacking and identity theft. Such an attack is known as Phishing Attack [20].

5.3. Classification of Threats

Threats can be understand as final potential loss for the system. They can be listed as:

5.3.1. Loss control over Resources

In cloud architecture, organizations handed over their sensitive business application and information to third party vendor. As a matter of policy, cloud provider does not provide transparency about its management policies i.e. how data was processed, transferred and where it is stored for security reason. Hence results in organization loss control over its sensitive resources [24]. Thus organization may require being very careful while moving sensitive resource over cloud or should define clause for its special request for control in *Service Level Agreement*.

5.3.2. Misuse of cloud computing resources

Presence of malicious users, employees and easily accessible management interface leads to misuse the resource to plant attacks over cloud computing [24]. It should be avoid via implementing strong encryption, verification, background check up and authentication techniques.

5.3.3. Malicious Insiders

With higher level of access, an employee should gain access to confidential data and services. In house activities are often bypassed by a firewall or *Intrusion Detection System* (IDS) assuming as legal activity. However, a trusted insider may be turn into adversary e.g. malicious insiders may access confidential data and gain control over the cloud services with no risk of detection [20]. Cloud provider should have a mechanism to scan the activities of their employee having higher level of access to read malicious action.

5.3.4. Account or Service Hijacking or Identity Theft

An account or service hijacking or identity theft can be defined as hacking of an account or service. It may be done via social engineering and or due to weak credentials. It allows performing malicious act such as access sensitive data manipulate data and redirect any transaction [10, 19, and 20].This brings the attention towards phishing attack, fraud, exploitation of software vulnerabilities, reused credentials [21].

5.3.5. Data Scavenging

Data for multiple users are stored at same location in cloud. It is possible data for multiple users may be stored at same disk space or multiple copies of data were created to ensure high reliability and increase trust over cloud. This would create problem for request of complete data deletion and open a space for malicious actors to steal sensitive data or information of a particular organization [19]. It is recommended for cloud user to mention a clause in *Service Level Agreement*, about the sensitivity of data or information to ensure appropriate security and privacy.

5.3.6. Data Loss or Leakage

Data in cloud is shared among multiple organizations. Hence may be in danger of his leakage or loss. It was leaked when transferred over internet (because of attack such as man-in-the-middle attack, ARP Spoofing), processed over internet (because of weak authentication and authorization mechanism) and stored over internet (because of poor isolation, incomplete deletion, disaster recovery provided by unreliable party, weak encryption algorithm). It should require timely audit of system performance, validation and testing [19, 20].

5.3.7. Denial of Service

Denial of service makes a significant impact on service availability metrics. It was caused by receiving large number of request from malicious host. Such type of cause is done via Zombie attack [19, 20].

5.3.8. Customer Data Manipulation

User attack web applications by manipulating data sent from application component to the server's application with help of SQL Injection, insecure direct object references and cross site scripting [19, 26-28]. Figure 3 shown mapping between vulnerability, attack and threats.

6. PURPOSE AND CONCLUSION

6.1. Purpose

The main focus was to understand the security domain in cloud architecture. Security is one of the biggest threats in cloud computing. The intension was to highlight three important pillars vulnerabilities, attacks, and threats and discuss about the strong correlation between them. Motive of study was to bring the intension of researcher to cure the loop holes as early as possible in cloud architecture.

6.2. Conclusion

This paper has discussed different vulnerabilities with corresponding attacks and threats. In the end strong correlation ship between vulnerabilities, attacks and threats was noticed. But it was also noticed that volume of researches focused on suggesting counter measures for different threats. As a conclusion this paper would like to bring the attention of all the academician and researchers to work on early detection of vulnerabilities in existing system to cure it from malicious attack and their corresponding impact threats.

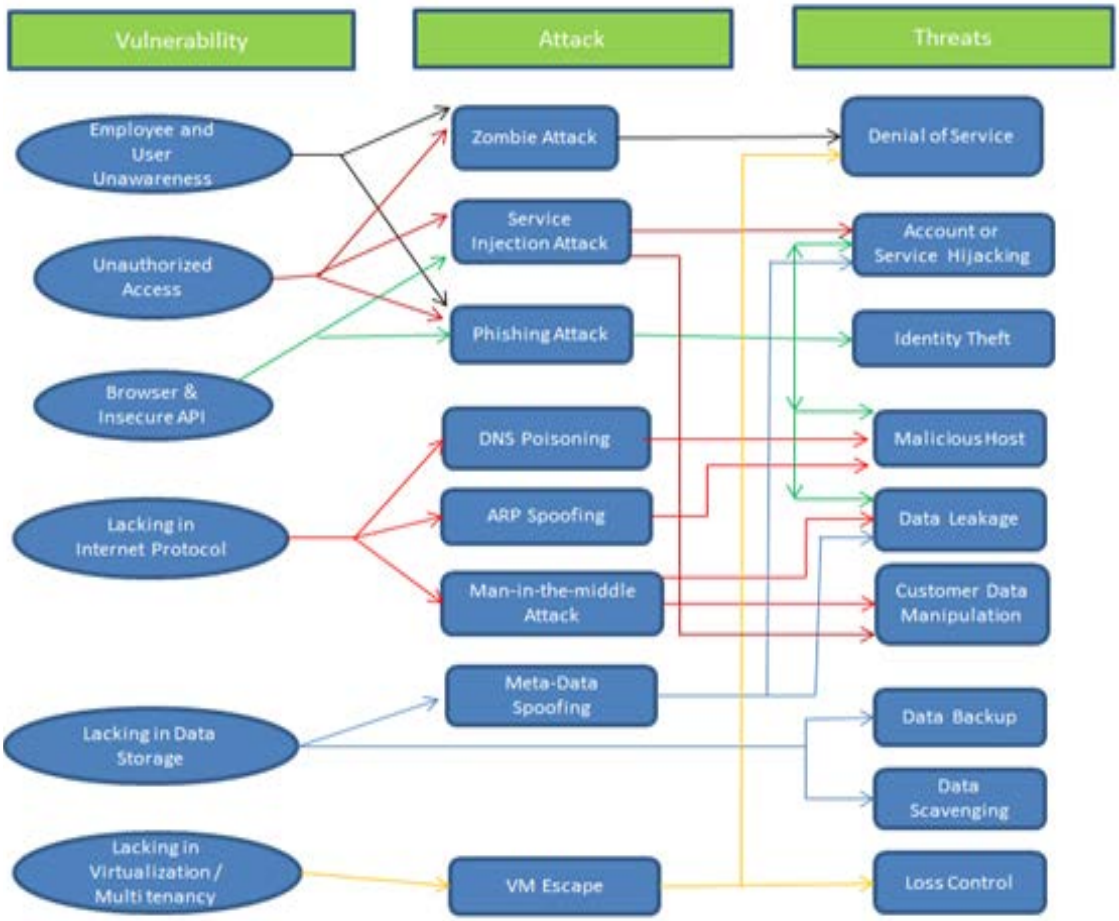

Figure 3. Mapping between vulnerability, attack and threats

ACKNOWLEDGEMENTS

This work is acknowledged under Integral University manuscript No IU/R&D/2017-MCN000111.

REFERENCES

[1] Gartner, "Gartner identifies the top 10 strategic technologies for 2011", "web reference": http://www.gartner.com/it/page.jsp?id=1454221, "Last access date": 02 Dec. 2016.
[2] Ponemon, "Security of cloud computing providers study", "web reference": http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf, "Last access date": 5 January 2017.
[3] J.H. Che, Y.M. Duan, T. Zhang, J. Fan, "Study on the security models and strategies of cloud computing", In proceedings of International Conference on Power Electronics and Engineering Application, Shenzhen, china, 2011, pp. 586-593
[4] A. Patel, M. Taghavi, K. Bakhtiyari, J.C. Junior, "An instruction detection and prevention system in cloud computing: A systematic review", Journal of Network and Computer applications, Vol. 36, no.1, 2013, pp. 25-41.
[5] Gens F, "New idc it cloud services survey: top benefits and challenges", "web reference": http://blogs.idc.com/ie/?p=730 , "Last access date": 23 December 2016.
[6] PayPal Outage, "web reference": http://royal.pingdom.com/2009/08/04/the-paypall-outage-cost-its-users-between-7-and-32-million-usd/, "Last access date": 13 January 2017.
[7] Sony Network Breach, "web reference": http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony, "Last access date": 20 January 2017.
[8] Window Azure Storage Disruption, "web reference": https://azure.microsoft.com/en-in/blog/details-of-the-february-22nd-2013-windows-azure-storage-disruption/, "Last access date": 31 January 2017.
[9] M. Peter, G. Timothy, "The NIST Definition of Cloud Computing", "web reference" "faculty.winthrop.edu/domain/csci411/Handouts/NIST.pdf", "Last access date": 28 Feb 2017.

[10] Cloud Security Alliance, "web reference": https://cloudsecurityalliance.org/research/top-threats, "Last access date": 15 December 2016.
[11] B.R.Kandukuri, R.Paturi, A.Rakshit, "Cloud Security Issues", IEEE International Conference on Service Computing", 2009
[12] M. Cusumano, "Cloud Computing and SaaS as new computing platforms", Communications of the ACM, vol. 53, no. 4, 2010, pp. 27-29
[13] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future generation computer system, vol.28, 2010, pp. 583-592.
[14] P. Saripalli, B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", IEEE 3rd International Conference on Cloud Computing, 2010.
[15] D.G. Feng, M. Zhang, Y. Zhang, Z. Xu, "Study on cloud computing security", Journal of Software, vol. 22, no.1, 2011, pp. 71-83.
[16] S. Subashini, V. Kavitha, "A survey on security problems in service delivery models of cloud computing", Journal of network and computer applications, vol.34, no.1, 2011, pp. 1-11.
[17] B. Joshi, A. Vijayan, "Securing cloud computing environment against DDoS attacks", In proceeding of IEEE International conference of computer communication and informatics, 2012.
[18] Z.Duan, P.Chen, F.Sanchez, Y.Dong, M.Stephenson, and J.Barker, "Detecting spam zombies by monitoring outgoing messages", IEEE transaction dependable and secure computing, vol. 9, no.2, 2012, pp. 198-210
[19] K. Hashizume, D.G. Rosado, E.F. Medina, E.B. Farnandez , "An analysis of security issues for cloud computing", IEEE, vol., 2013
[20] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, "A survey on security issues and solution at different layers of cloud computing", IEEE, vol. 63, 2013, pp. 561-592
[21] J. Chhikara, R. Dahiya, N. Garg, M. Rani, "Phishing & Anti Phishing Technique: Case Study", International Journal of Advanced Research in computer science and software engineering, vol. 3, no. 5, 2013, pp. 458-465.
[22] K.A. Torkura, F. Cheng, C. Meinel, "A Proposed Framework for Proactive Vulnerability Assessment in Cloud Deployment", the 10th International Conference for Internet Technology and Secured Transactions, 2015
[23] M. Masky, S.S. Young, T.Y. Choe, "A Novel Risk Identification Framework for Cloud Computing Security", IEEE Transaction, 2015.
[24] D. Niu, L. Liu , X. Z. Zhang, S. Lii, Z. Li, "Security Analysis Model, System Architecture and Relational Model of Cloud Services", IEEE, Vol. 13,2016,pp.574-584
[25] Rakshita C M, "Zombie attack detection and counter measure selection in cloud environment", International Journal of advances in electrical power system and information technology, vol. 2, no.4, 2016, pp. 24-28.
[26] B. Indrani, E.Ramaraj, "An Approach to detect and prevent SQL Injection Attacks in database using web services", International Journal of computer science and network security, vol.11, 2011, pp. 197-205
[27] B. Indrani, E.Ramaraj, "Prevention of SQL Injection attacks by using service oriented authentication technique", International Journal of modeling and optimization, vol. 3, no.3, 2013, pp. 302-306
[28] R. Shrivastava, J. Bhattacharyji, R. Soni, "SQL Injection Attacks in Database using web services: Detection and prevention- Review", Asian Journal of computer science and information technology, vol.2, no.6, 2012, pp. 162-165
[29] King S, Chen P, Wang YM, "Subvert: implementing malware with virtual machines", in: IEEE Symposium security and privacy, 2006, pp. 314-327.
[30] Rutkowska J, "Subverting vistatm kernel for fun and profit". In: Black Hat Conference, 2006.
[31] Bahram S, Jiang X, Wang Z, Grace M, "Dksm: Subverting virtual machine introspection for fun and profit", in: Proceedings of the 29th IEEE international symposium on reliable distributed system, 2010
[32] Metz C, "DDoS attack rains down on amazon cloud", "web reference" "http: // www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/, "Last access date": 28 Feb 2017
[33] Popovick, HocenskiZ, "Cloud Computing Security issues and challenges", In: Proceedings of the 33rd International convention MIPRO IEEE Computer Society Washington DC, USA, 2010, pp. 344-349.
[34] Pauli D, "Amazon's ec2, eucalyptus vulnerability discovered", "web reference": http://www.crn.com.au/News/278387,amazon-ec2-eucalyptus-vulnarability-discovered.aspx, "Last access date": 15 January 2017.

BIOGRAPHIES OF AUTHORS

Shaz Alam completed his graduation BSc. (CPM) from Lucknow University and post-Graduation MSc. Tech (IMCA) from Jamia Millia Islamia New Delhi. Right now pursuing PhD (Cloud Computing) in Department of Computer Application from Integral University Lucknow and has 5 year of experience as Corporate Trainer in Center for Career Guidance & Development Integral University Lucknow. His area of interest includes Cloud computing, Java technology, and Formula independent approaches. Integral University Department of Computer Application Lucknow -226026, UP, India shaz.alam62@gmail.com

Dr. Mohd. Muqeem has completed his doctoral from Integral University, Lucknow. He is presently working as Associate professor in the Department of Computer Application Integral University Lucknow. He has more than 14 year of experience in the field of Academics. He is currently working in the area requirement engineering and web technologies. He has published paper in reputed journal with impact factor. He is a member of CSI, ISTE, CSTA, IAENG and other societies. Integral University Department of Computer Application Lucknow 226026, UP, India. muqeem.79@gmail.com

Dr. Suhel Ahmad Khan has earned his doctoral degree from Babasaheb Bhimrao Ambedkar University, (A Central University), Vidya Vihar, Raibareli Road, Lucknow. He is currently working as an assistant professor in the Department of Computer Application, Integral University, Lucknow, UP, India. Dr. S.A. Khan is a young, energetic researcher and has completed full time major project funded by University Grant Commission, New Delhi. He has more than five years of teaching and research experience. He is currently working in the area of software security and security testing. He has also published and presented papers in refereed journals and conferences. He is a member of IACIT, UACEE and Internet Society. Integral University Department of Computer Application Lucknow -226026, UP, India ahmadsuhel28@gmail.com