International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 22 (2018) pp. 16077-16084

Cloud Computing and Security Issues—A Review of Amazon Web Services

Abdullah Alqahtani, Hina Gull

Department of Computer Information System, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam Saudi Arabia.

Abstract

Cloud Computing has evolved as a popular and successful discipline with the present-day advancement in technology. Nowadays, new business jargon has witnessed an immense success by deploying their services and data on web without depending on any of the physical maneuver. This independence and trend have driven many renowned companies such as Netflix, Salesforce and Amazon towards cloud-based infrastructure Amazon web services (AWS) overshadows the market for offering cloud-based services with top metrics like huge volume, flexibility, availability and large number of customers. However, in addition to several benefits offered by the cloud infrastructure of Amazon (AWS), cloud security remains as the major point of concern for Amazon. In this review paper, we have described some of the common security concerns faced by a common cloud infrastructure. But the focal point of this review paper is the security vulnerabilities of Amazon Web Services, which are proved to be a kind of barrier for widespread use of Amazon Web Services (AWS).

Keywords: Cloud Computing, Amazon Web Services, Cloud Security, Privacy, Database Encryption

1. INTRODUCTION

The term *cloud computing* refers to a method through which information and programs can be stored and accessed without storing or accessing it on any physical media. This is highly advantageous to companies that require large amount of disk space. It is a modern means to save internal IT resources, because data is not stored in-house. Rather, data is stored in a "cloud" from where it can be retrieved anytime. In today's modern world, using cloud computing helps large corporations to make huge savings. This is because they do not need to worry about financing the required software or hardware. Instead, they simply choose a cloud service and obtain the required software or hardware in a few clicks. This is overall a far more economic and fast process compared to traditional methods of storing and accessing data [1].

Cloud Computing provides three kinds of services:

i) Private cloud: This type of cloud owned by the organization is meant to provide services to its own users.
ii) Public cloud: Third party are providing the services. Examples include Amazon Web Services (AWS), Microsoft Azure, IBM/SoftLayer and Google Compute Engine.
iii) Hybrid cloud: This is a combination of services provided by private and public clouds. The main goal of this kind is to achieve scalibility.

Cloud computing has three categories of services:

i) Infrastructure as a service: It helps users to transfer work from one machine to another, usually a virtual machine.
ii) Platform as a Service: PaaS is used for general software development. Common PaaS providers include Salesforce.com's Force.com, Amazon Elastic Beanstalk, and Google App Engine.
iii) Software as a service: SaaS delivers software applications over the Internet; these are often called *Web Services*. Microsoft Office 365 is an example of an SaaS.

There are many examples of cloud computing services, including Google drive, Apple iCloud, Dropbox, SugarSync and AWS. Examples of cloud service providers for each cloud service model have been given by [2] and are shown in Figure 1.

Cloud Service Models	Cloud Service Providers
SaaS	Antenna Software, Cloud9 Analytics, CVM Solutions, Exoprise Systems, Gageln, Host Analytics, Knowledge Tree, LiveOps, Reval, Taleo, NetSuite, Google Apps, Microsoft 365, Salesforce.com, Rackspace, IBM, and Joyent
PaaS	Amazon AWS, Google Apps, Microsoft Azure, SAP, SalesForce, Intuit, Netsuite, IBM, WorkXpress, and Joyent
IaaS	Amazon Elastic Compute Cloud, Rackspace, Bluelock, CSC, GoGrid, IBM, OpenStack, Rackspace, Savvis, VMware, Terremark, Citrix, Joyent, and BluePoint

Figure 1: Examples of cloud service providers with respect to cloud service models

1.1. Security issues with cloud computing services

A study in [3] have discussed security risks, vulnerabilities, and attacks, with reference to overall networks in general and cloud computers. Among many security attacks, the authors found that the there are several types of attack on cloud computers affecting their confidentiality, integrity, and availability. The most common type of attack is the *denial of service* (DOS) [4]. A DOS attack makes a given cloud owner's resources unavailable to them and their users. The authors explain that a security flaw in a cloud infrastructure can have more devastating effects, because hardware and other resources are shared on a cloud. A breached system can spread its effects to other systems that might belong to someone else using the same

cloud storage. Hence, it potentially impacts a large population [5]. Some of the security attacks, like finding encryption keys, getting to know about plain text, and other cryptographic attacks affect only the machine owner's data. They have lesser or no effect on other cloud server users [6].

One of the biggest security risks involved with cloud computing is the element of trust. This is because the service user is not buying, configuring, monitoring, and implementing their own personal computers and servers physically. These services are provided to them on request by a cloud computing service provider. This makes their configuration and internal settings vulnerable to the services on which they rely. This situation can lead to an attack on the confidentiality and/or integrity of the data present in the cloud [7].

In [8], the authors have elaborated on the significant risks involved with cloud services in particular. As a result, the authors have provided some solutions related to security concerns for industries and cloud computer service providers. The security concerns include secure data transmission, encryption, access controls, authorization and authentication, customer service, data privacy, log monitoring, intrusion detection, and auditing. Besides these, proper risk management procedures must be followed by cloud providers.

Strategies, measures, and rules should be created, recorded, and executed. Training materials or courses should be produced that set a standard for giving basic security and risk administration abilities and education to the cloud computing suppliers, the security group, and their internal partners.

1.2. Amazon Web Services

Although there are many types of cloud computing services, the cloud services provided by Amazon, known as Amazon Web Services (AWS), has gained special attention over the past few years. This can be demonstrated from various fact sheets and surveys. In 2014, research conducted by Synergy Research Group showed that the market share of AWS in the cloud infrastructure market had risen exponentially in the previous five years (Figure 2) [9]. A survey conducted by Synergy Research Group in 2016 [10] declared AWS as the leading cloud service provider. The rapid growth of AWS can clearly be seen by the market it controlled in 2015 (Figure 3). Parker Thomas in [11] indicated that in 2015, AWS had reached up to 35% of market share. (Figure **4**). It can be concluded that AWS plays a leading role among all the cloud service providers. When more people use a service having security flaws, more people are prone to suffer from these flaws. Hence it can be stated that, with this rapid growth of AWS, it is of the utmost importance to gather information about any security issues with the platform. The need of understand the security requirements and deficiencies of AWS cannot be avoided in today's world. This paper provides a review of security research in the field of cloud security with respect to AWS. It is also intended to act as a source for building a strong knowledge base for future researchers regarding the security situation, flaws, and vulnerabilities related to AWS.

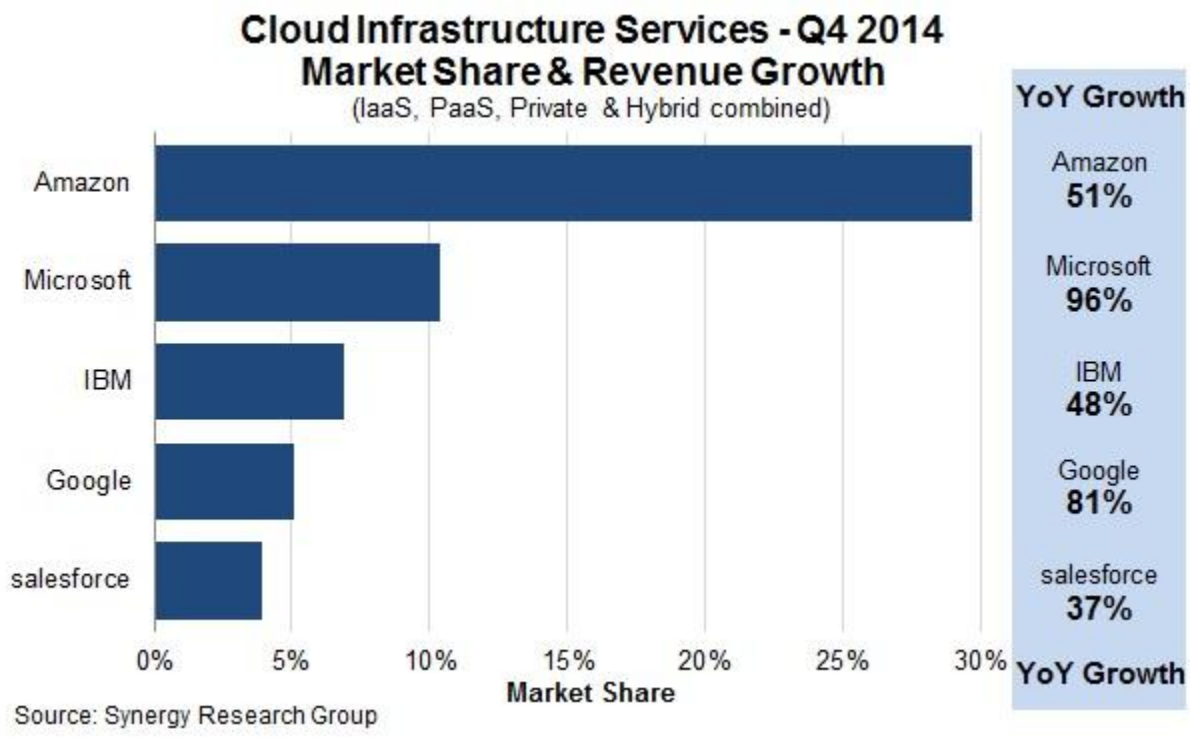

Figure 2: Survey conducted by Synergy Research Group

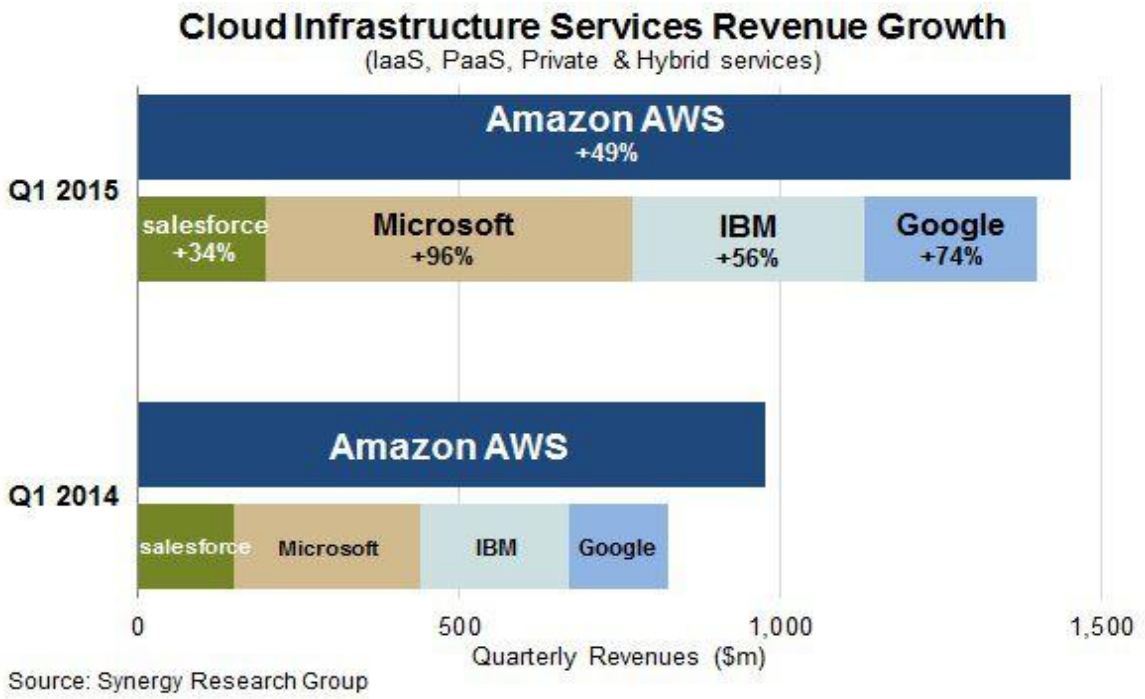

Figure 3: Survey conducted by Synergy Research Group

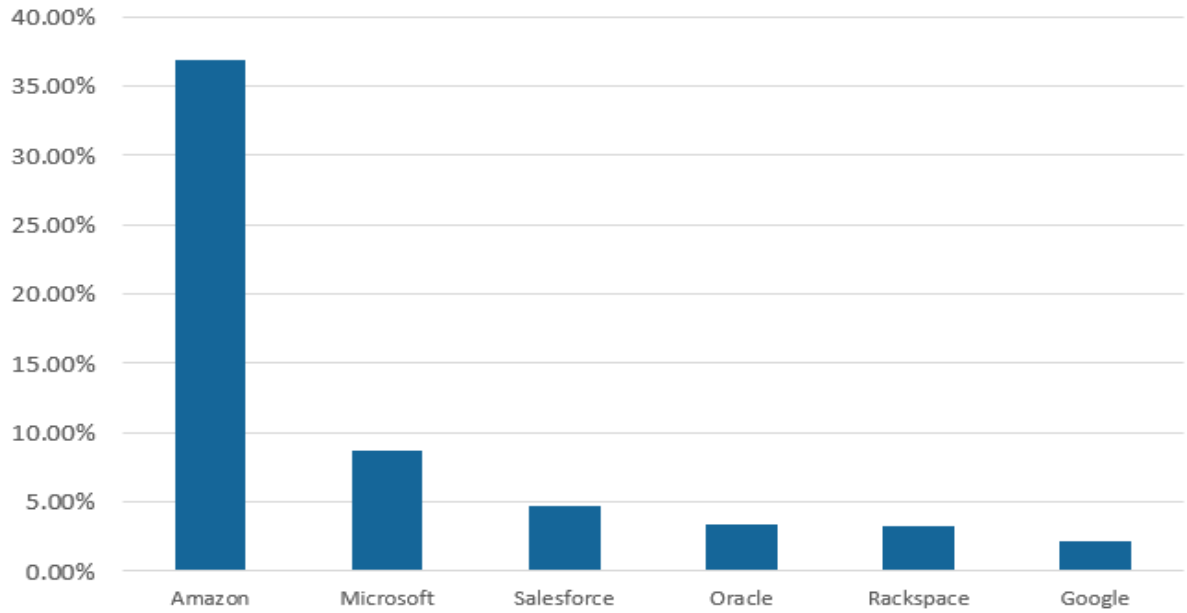

Figure 4: Cloud platform market share [11]

2. LITERATURE REVIEW

In a study [13], the authors selected Amazon EC2 instances, and used them to show the methods of gaining access to and exploiting an instance. Also, in [14], the authors showed that cloud clients are not watchful when picking EC2 instances. By distributing a malicious instance, they observed that this instance was started a few times and that data about the use of the instances could be gathered. In addition, they demonstrated that it was possible to evade the payment mechanism of paid images by changing the AMI file.

The authors in [15] used graph theory techniques to study security issues associated with Amazon EC2 with respect to the configuration of images. The authors provided various security recommendations that are applicable at the infrastructure level of AWS, rather than at instance level.

The authors in [16] researched security issues associated with images on the Amazon EC2 Service. An automated system was created by the authors. Various tests were done in order to achieve the desired results. The system tested if the programs used in images are up to date or not. The system was also used to test common vulnerabilities in various operating systems like Windows and Linux. Nessus [25] was used for this purpose. The results indicated that clients and providers of public images can both suffer from the dangers of potential security weaknesses present in EC2. Most of the software programs used were updated two or more years ago. 98% of Windows AMIs and 58% of Linux AMIs contained software with critical vulnerabilities. The associated security risks include loss of privacy, authority, and system infections through malware. Another test was performed to investigate the probability of compromise of cloud systems through malware. ClamAV [26] was the anti-virus software used for this purpose. The results indicated that Windows machines are more vulnerable to internet malware compared to Linux systems. The results also indicated that EC2 had no mechanism to differentiate connection of a legitimate source from a malicious source; also that, if clients using a particular image has not removed their credentials fully from that machine, there were ways to recover full credentials using various tools available online. Anyone renting the image subsequently could gain access to credentials, and then use AWS with the original client being billed. This study concluded that there must be appropriate vulnerability assessment before renting and using a cloud-based image.

The authors in [17] clarified the shortcoming of AWS regarding security services in 2013. Netflix leases space from Amazon Web Services (AWS) to operate membership administration to watch their movies and TV episodes. As indicated by the investigation of information leakage of 209 worldwide organizations in 2011, 37% of information leakage cases included malicious attacks.

In 2012, a retailer owned by AWS, known as Zappos, was the victim of cyber theft [18]. The number of clients whose login information might have been leaked is up to 24 million.

In [19], the authors evaluated an ordinary environment of the mainstream AWS cloud with a focus on security. The cloud security was surveyed by implementation of Dionaea honeypots for a couple of months in the given systems. In the experiment done by authors, three AWS EC2 instances ran in parallel in the regions of Singapore, US East Virginia, and Sao Paulo. An overall comparison was also provided among the three regions. The results are shown in Table 1.

Information and logs gathered from Dionaea honeypots demonstrate that the cloud security environment is shockingly weak and needs to be improved. The results demonstrate that cloud suppliers don't provide security and data assurance to cloud clients, and this requires the cloud clients to secure and assure their own data. Cloud clients need to take fundamental measures to secure the applications and administration that they host, or plan to host, on the cloud.

Table 1: Results of experiment done by Eman Al Awadhi Khaled Salah Thomas

	Singapore	**US East Virginia**	**Sao Paulo**
No. of connections	53,795	69,067	33,687
Max connections from single IP address	23,709	36,517	9792
No. of times malware infection occurred	7642	21	11

Later in 2013, the main purpose of [20] was to conduct an analysis of AWS clouds in terms of the arrangement of current security standards, and to identify potential issues with acquiring "trustable security controls" in compliance with various security standards, such as DoD, ISO 27001, HIPAA etc. The authors concluded that AWS fails to explain to the clients what exactly they are allowed to do. There are no mechanisms for non-repudiation, risk assessments, user access, controlled access points, unauthorized persons entry, asset management, background screening, user access policy, user access restriction/authorization, user access revocation, incident management, antivirus/malicious incidence response and reporting, audit logging, IDS, and Customer access requirements.

In [21], the authors depicted some essential security issues that were compelling to cloud services in 2014. The authors examined different perspectives on cloud security, including information security, cloud dangers, cloud administration, and account hijacking. Attackers were successful in establishing an XSS hijacking attack on AWS in 2010. Amazon Relational Database Service (RDS) was also attacked such that, even if they lost their unique access, the attackers would still have a backend into the Amazon framework. The attackers were able to obtain the login data of any individual who clicked the login button on the Amazon landing page. The attackers utilized their servers to contaminate new machines with the Zeus trojan malware [29] and control machines effectively tainted with it. This contextual investigation uncovers a vital conclusion: that even one flawed security framework may compromise an entire system. The authors concluded by proposing two solutions to such attacks on AWS. First of all, AWS should not allow services and clients to share account login information with each other. Secondly, a two-factor authentication scheme (something you know and something you have) is proposed. The authors explain the security situation of AWS. They explain that all the computers involved in AWS were audited and compliant to 20 security standards including ISO 27001, HIPAA, DoD CSM, and PCI DSS. However, despite the assertion that all the necessary security updates and patches were in place, various studies have shown that there are still some security loopholes in AWS.

The authors in [22], in 2015, discussed the problems associated with the specific vulnerability assessment process for cloud computers. The study found that cloud vulnerability assessment methodologies usually focus on finding vulnerabilities in IaaS. Lesser importance is given to security as a service. According to the authors, this is also a very important aspect in cloud computing and must be assessed for vulnerabilities, since more cloud specific threats and vulnerabilities are emerging day by day. The proposed vulnerability assessment approach offered by the authors was based on AWS. It is known as CAVAS. It was deployed on Amazon Linux and Ubuntu images. The database used was enhanced to make it accessible from EC2 and local systems through command line interfaces. The authors claim that their CAVAS model has the ability to monitor, gather, and correlate vulnerability information from various resources. OpenVas [28] was also integrated with CAVAS. In order to make the vulnerability assessment results more reliable, more security related information was programmed into CAVAS using the NESSUS scripting language. On the occurrence of an event, their framework gives severity ratings of the event. OpenVas wrongly recognized Amazon Linux (as CentOS) and was unable to distinguish RDS establishment. From these outcomes, we find that CAVAS creates more precise filtering results for cloud applications. This work delivers a first phase in recognizing and eliminating these sorts of AWS security vulnerabilities.

Nicholas Serrano et al. [23] examined the latest technologies associated with and utilized by the cloud market in 2015. Among others, two of the major technologies considered were security and its monitoring. According to the authors, it is very important to enforce secure firewalls and patched operating systems along with up-to-date configurations of applications. The authors stress securing each entity in a cloud based environment, because a single security flaw can lead to compromise of the complete infrastructure. According to the author, AWS gives users the ability to operate systems independently. While it seems convenient for the user, it may give rise to security issues for a wider group. AWS offers technical support, but only on premium membership tariffs. This makes AWS a not very cost effective or reliable service if a security incident occurs.

The fundamental point of [24], in 2015, is that cloud computing security should be a core operation and not an additional service. AWS is *the* distributed computing supplier. It is a reference case of genuine cloud computing which offers excellent cloud administration as well as providing security for its clients' information. IT assets are accessible at very low cost and no additional payment is required for the assets and resources. With AWS cloud services, one can set up a huge number of servers immediately. Henceforth AWS permits great improvement and organization of an application. The authors also focus on the security aspect of AWS services. In order to provide security to clients, AWS hires professional security staff. In order to protect systems from intrusion, CCTV cameras, intrusion detection systems, and patched programs are installed. Physical security is also assured by ensuring no strangers enter the building. AWS includes secure transmission controls, network architecture, access points, and monitoring services. Secure protocols are used like HTTPS instead of HTTP. According to the authors, as a consequence of all these security controls and mechanisms, clients trust AWS.

3. DISCUSSION

This research paper focuses on security issues faced by AWS in the span of nine years (2009–2016). Throughout these years, various research has been conducted. Only the most reliable and well-known works have been discussed. With time, the security conditions of AWS have improved. Authors in [14] demonstrated the possibility to evade the payment mechanism of paid images by changing the AMI file. The authors in [16] have researched about security issues associated with images on Amazon EC2 Service. These images are preinstalled virtual machine images called as AMI. Authors have developed a system which is used to perform the security evaluation of Amazon AMI automatically. Number of experiments were conducted over a span of five months. The results indicated that clients and providers of public images can both suffer from the dangers of potential security weaknesses present in EC2. Following are the details of security vulnerabilities found in AMI:

Malwares: Authors claimed a huge number of malwares such as viruses, Trojan horses, spyware and worms were detected while experimentation and evaluation. Most dangerous malware found was Trojan horse commonly known as Trojan-spy containing dangerous abilities such as stealing sensitive information and files, performing different kinds of key logs and monitoring the computers. This malware also has capability to record and change the browser history. During manual evaluation, it was observed that this kind of malware is changing browsers setting, can do decryption and password recovery.

Unsolicited Connections: While experimentation, several open connections through several images were observed. It was found very difficult to find out the real connection with AMI. In other words, there was no method found to differentiate between the real and the malicious connection. By closely analyzing the experimentation results, several unwelcomed connections were opened by AMI resulting into serious security vulnerability.

Backdoors and Leftover credentials: When a user rent an AMI, he has to provide the public part of his ssh key. This key is then stored by Amazon in their open home directory, which being opened can be accessed by anybody. The problem with this process is that if the user is fake or spiteful, he intentionally does not remove his key from the image. In turn, that spiteful user before declaring his key as public and can get access to any running instance of the image. Though these ssh servers apply password authentication process, but same backdoor trick can be applied to these passwords, if AMI providers intentionally or by mistake keep their passwords on the machine. By using these backdoors, anybody can excerpt the traces of the passwords, which can then be cracked by using third party software. Through experimentation the possibility of these leftovers was found to be about 21.8% which raises main security concern for Amazon.

While sharing the AMIs, authors also mentioned some of the privacy concerns and risks associated with these AMIs. Especially if these images contain the sensitive information it may be available to anybody. Authors concluded that 22% of the analyzed AMI contained information in their last login database. Similarly looking and analyzing the browser and shell history can also lead to privacy breaches.

In [17], the authors have indicated the shortcoming of AWS regarding its security provision. According to their study, in 2011, 209 countries suffered from information privacy issues. A study in [18] shows that the number of AWS clients whose private information was leaked was almost 24 million. Eman et al [19] inspects the security of Amazon AWS cloud by deploying Dionaeo honeypots at different regions. Honeypot is the copy of real network, specially designed with some security loopholes and vulnerabilities. In short, it is a kind of trap to find malwares and hijackers attack on AWS. Honeypots were deployed at three main regions Virginia, Singapore and Sao Paula. All three AWS EC2 instances were made to run in parallel in order to reveal complete type and number of strikes by the attackers. Honeypots were also used to find the kind of malicious software used by the attackers. Authors have analyzed the results in each region. According to the comparative study among all three regions, it was found that Sao Pulao was at the top in receiving in receiving malicious connection attempts followed by Singapore and Virginia. Also authors are of the opinion that attackers are able to inject malicious software into the system through infected URLs. Same order as of malicious connections was followed in infecting URLs i.e. Sao Pulao, Singapore and Virginia are attacked through infected URLs respectively. Even attackers are found to be from different countries and regions. Their detailed experimentation and study put a question mark on the security of AWS cloud. In the end, the authors concluded that AWS cloud clients need to take fundamental measures to secure their applications and administrations that they host or plan to have on the cloud.

Compliance of security and privacy standards are one of the most important areas in providing the open cloud services. To protect user privacy and security, cloud providers are normally giving security and privacy control to their customers. But there is always a need that these cloud providers enable their users to follow the set security standards to achieve transparency. Authors in [20] have taken AWS as a case study and have compared security services provided by Amazon with the set standards. After a profound research done by the authors showed several security mechanisms were lacking in AWS or they are not complying the security standards.

The authors in [21] depicted some essential security issues that are compelling to cloud services in 2014. Services and account hijacking was considered as a serious risk during the development of a cloud. Hijacking of services and account entails to unauthorized access to the credentials of the users and impermissible use of the services rented out by the clients. Authors mentioned that the AWS cloud was preyed by the attackers via use of hijacking technology. A normal attack by use of cross site scripting (XSS) led to a massive security and privacy breach of AWS cloud. Hijackers, by this simple way not only gained access to the AWS credentials but also recorded the traces of Amazon Rational Database (RDS), providing them with the backend Amazon services. Even if they lose the original access, still they have access to the backend services of AWS. Widely used malware called as Zeus Trojan was used by attackers to get control over the Amazon machines. All the computers that are infected by this Trojan attacked began to ask for instructions and updates from Amazon. It was considered as the Amazon fault having security vulnerability at one site, leading to a humongous security breach all over the network of AWS in just short span of few months. The authors concluded by proposing two solutions to such attacks on AWS. First of all, AWS should not allow services and clients to share account login information with each other. Secondly, a two-factor authentication scheme was proposed. However, both these solutions don't seem to be good enough for the users or clients; leading to bad usability, slow output and burden on their pockets. Multifactor authentication also requires the user to have knowledge and possession. Even if users are not sharing their credentials and login information directly, Amazon has to provide them with third part communication channels between users and AWS, causing out of budget constraints.

The authors in paper [22], in 2015, have discussed the problems associated with cloud computers specific vulnerability assessment. The study found out that the cloud vulnerability assessment methodologies usually focus on finding vulnerabilities in IaaS. Lesser importance is given to security as a service. Authors came to the conclusion that current measures for the identification of cloud vulnerabilities are not good enough. This proves to be one of the major causes for not identifying the potential security hazards faced by AWS cloud. As AWS cloud is mainly dealing with web services, so there is a need of a proper framework which not only assess the security issues in IaaS, but also take SaaS into proper account.

In this paper [23], the author examined AWS and concluded that it offers technical support but only on premium membership. Hence, the clients who do not pay for a premium membership, do not get desired security features; thus, exposing them to malicious security threats.

Fabio et al [30] has taken an important issue of database security in the Amazon Web Services cloud. They have taken the concern of SaaS applications into account that normally SaaS applications are in a need to transfer data and other required resources to the cloud, that gave birth of number of issues such as protection of privacy, proprietorship and data. Authors have mentioned a main gap in the infrastructure of AWS that they don't provide adequate encryption key support to the data. Using Vetiver (a home health care SaaS application) as a case study, authors have figured out several challenges faced while deploying this health care application on AWS cloud. Authors after analyzing the requirements for secure healthcare applications believe there is a special need of IT and security standards for healthcare SaaS applications especially when they have to be deployed on AWS cloud infrastructure. Authors mentioned the special concern of providing partial solution for data security provided by AWS, leading an overhead of data protection on cloud consumers. As a result, cloud consumer has to buy, install and configure security solutions by themselves with less support. Following are some of the challenges that AWS cloud providers face when they

have to make their cloud infrastructure feasible for deploying applications containing highly sensitive data:

Cloud environment is shared by several SaaS application providers, each SaaS provider has some special privilege for their data access and reach, but still confidential data should be protected from SaaS as well as AWS providers. They proposed the use of encryption method that will not only protect the data from malicious SaaS applications but also from the spiteful cloud providers.

Another major issue is the management of the keys. As encryption is based on keys which are used to encrypt and decrypt data, key management (which includes key generation, storing keys and renewal) should also be done in a protected way.

Third major issue is the protection of key stores not only from the malicious users but also from the key loss, which will in turn lead to the loss of data protected by these keys.

Authors in their proposed an architecture provide better security by providing at-rest data encryption for SaaS systems [12], in addition to a key management subsystem for key generation, renewal and protection. Later, proposed architecture is implemented by applying encryption to the sensitive data stored in the database.

CJ Radford [31] in his article on data protection issues faced by Amazon Web Services believes that, though AWS hold the market for their reliable cloud based infrastructure as they are providing layered based security within its management and the network environment, still there is a loophole of providing reliable data protection in EC2 and EBS. He has mentioned number of issues related to data protection and discussed their solutions which are as follows:

Major data breach hazard posed on AWS is by their own privileged users who has complete access not only to snapshot of EC2 instance but also to the data it contains. If the account is used by some spiteful users, data will be exposed to the outsiders. EC2 and EBS provides security against the overall network access to the instances but are no paying any attention towards the data accessibility within AWS instance.

To prevent these issues there must be strong laws and centrally controlled policies to decrypt the data at file system level. There should also be restrictions in the privilege and permission granted to the users. Least access to data should be given to the students only at a time when they need data. Even the privileged users should perform all data management and related functions without seeing the tables that are protected. In other words, strong encryption with strong key management should be provided to the users. It is also the need of the hour that network and data security roles should be separated from each other. All these measures should be directly applied to AWS cloud to protect data and the whole cloud.

4. CONCLUSION

The world congress on Internet Security survey [8] in 2013 indicated that there is always going to be a high demand for products providing security management. Since AWS gives its clients full control of an instance, it can be concluded that security is not only the responsibility of the cloud provider, but also of the client. Human beings are the weakest link, as they say. Another possible solution to the above-mentioned security issues can be that AWS should not allow services and clients to share account login information with each other. In addition, AWS users must read the tips and techniques for how to secure AWS [27] before starting to use the service.

REFERENCES

[1]. "How Cloud Computing Works", [Online]. Available: http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm

[2]. Te-Shun C., 2013, "Security Threats on Cloud Computing Vulnerabilities", *International Journal of Computer Science & Information Technology* (IJCSIT) Vol 5, No 3.

[3]. Mosca, P., Zhang, Y., Xiao, Z. and Wang, Y. (2014) Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. International Journal of Communications, Network and System Sciences, 7, 529-535.

[4]. Mutch, J., "How to Steal Data from the Cloud", 2010, [Online]. Available: http://www.cloudbook.net/resources/stories/how-to-steal-data-from-the-cloud

[5]. Archer J. (2010), "Top Threat to Cloud Computing", Cloud Security Alliance. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6]. Kirchgaessner S. (2013), Cloud Storage Carries Potent Security Risk, [Online]. Available: http://www.ft.com/cms/s/0/4729ed7c-3722-11e3-9603-00144feab7de.html

[7]. Simonite T (2012) "How to steal data from your neighbor in the cloud". MIT Technology Review, 8 Nov 2012. www.technologyreview.com/news/506976/how-to-steal-data-from-your-neighbor-in-the-Cloud/

[8]. Hanim. E. (2013), "Security threats and solutions in cloud computing," in *2013 World Congress on Internet Security, WorldCIS 2013*, 2013, pp. 139–143.

[9]. "AWS Market Share Reaches Five-Year High Despite Microsoft Growth Surge", (2015) [Online]. Available: https://www.srgresearch.com/articles/aws-market-share-reaches-five-year-high-despite-microsoft-growth-surge

[10]. Sullivan B. (2016). "Amazon Web Services Public Cloud", [Online]. Available: http://www.techweekeurope.co.uk/cloud/cloud-management/amazon-web-services-public-cloud-185687

[11]. "Can AWS Microsoft reach 50 market share cloud", (2015), [Online]. Available: http://marketrealist.com/2015/11/can-aws-microsoft-reach-50-market-share-cloud/

[12]. Cusumano M. 2010, "Cloud computing and SaaS as new computing platforms". Communication. ACM 53, 4 (April 2010), 27-29. DOI: https://doi.org/10.1145/1721654.1721667

[13]. Ristenpart T., and Savage S., 2009, "Hey, you, get out of my cloud: exploring information leakage in third-party compute clouds", In Proceedings of the 16th ACM conference on Computer and communications security.

[14]. Haroon M. and Nick A., 2010, "Clobbering the cloud", defcon.org, Communication Inc, U.S.

[15]. Bleikertz S., Probst P. and Eriksson K 2010, "Security audits of multi-tier virtual infrastructures in public infrastructure clouds", In Proceedings of the 2010 ACM Workshop on Cloud Computing Security, p. 93

[16]. Balduzzi M., Zaddach J., Balzarotti D., Kirda E., 2012 "A Security Analysis of Amazon's Elastic Compute Cloud Service", in *Proceedings of the 27th Annual ACM Symposium on Applied Computing - SAC '12*, p. 1427.

[17]. Te Shun C., 2013, "Data Breach Trends & Stats, Symantec", In *Proceedings of International Journal of Computer Science & Information Technology* (IJCSIT) Vol 5, No 3.

[18]. "He has Delivered Her First Giant Data Breach" 2012, [Online]. Available at http://www.infosecisland.com/blogview/19432-2012-Has-Delivered-Her-First-Giant-Data-Breach.html

[19]. Al Awadhi E., Salah K., Marti T , 2013, "Assessing the Security of the Cloud Environment", in *2013 7th IEEE GCC Conference and Exhibition, GCC 2013*, pp. 251–256.

[20]. Chemerkin Y., 2013, "Limitations of Security Standards against Public Clouds", Technical Co-Sponsored by IEEE Toronto Section i-Society 2013 Proceedings Contents, International Conference on Information Security.

[21]. Mosca P., Zhang Y., Xiao Z., Wang Y., 2014, "Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services", International Journal of Communications, Network and System Sciences, Vol.7 No.12

[22]. Torkura K. and Meinel C., 2016, "Towards Cloud-Aware Vulnerability Assessments ", In Proceedings of 11th International Conference on Signal Image Technology & Internet Based Systems, pp. 746–751.

[23]. Serrano N., Gallardo G., and Hernantes J., 2015, "Infrastructure as a Service and Cloud Technologies", IEEE Softw., vol. 32, no. 2, pp. 30–36.

[24]. Narula S., Prachi M., Jain A., 2015, "Cloud Computing Security: AWS", In Proceedings of Fifth International Conference on Advanced Computing & Communication Technologies.

[25]. "Nessus", [Online] Available: http://www.tenable.com/products/nessus/select-your-operating-system

[26]. "ClamAV", [Online] Available: https://www.clamav.net/downloads

[27]. "How to secure your Amazon EC2", Amazon Inc. about Amazon web services, [Online] Available: http://aws.amazon.com/articles/1233/

[28]. "OpenVas", [Online] Available: http://www.openvas.org/

[29]. "Zeus Malware", [Online] Available: https://en.wikipedia.org/wiki/Zeus

[30]. Bracci F., Corradi A. and Foschini L., 2012, "Database security management for healthcare SaaS in the Amazon AWS Cloud," *2012 IEEE Symposium on Computers and Communications (ISCC)*, Cappadocia, pp. 000812-000819.

[31]. Radford C.J., 2014, "Challenges and solutions protecting data within Amazon Web Services, Network Security", Volume 2014, Issue 6, June 2014, Pages 5-8, ISSN 1353-4858, http://dx.doi.org/10.1016/S1353-4858(14)70058-3.

Biographical Sketch:

Dr. Abdullah Alqahtani: Abdullah A. Alqahtani is assistant professor at the College of Computer Science and Information Technology; Imam Abdulrahman Bin Faisal University, Saudi Arabia. His main research interests include privacy, decision support systems, e-services, e-business, e-government, group decision making, resource planning, database design and development, system modeling, web-based information systems, intelligent decision support systems, data mining; business intelligence and system evaluation.

Ms. Hina Gull: She has done her MS in Computer Software Engineering from National University of Science and Technology, Pakistan. Nowadays, she is working as lecturer in Imam Abdulrahman Bin Faisal University Dammam Saudi Arabia. Her research interest includes Software Engineering, Human Centered Design and Algorithms.