American Journal of Information Science and Computer Engineering
Vol. 5, No. 2, 2019, pp. 38-46
http://www.aiscience.org/journal/ajisce
ISSN: 2381-7488 (Print); ISSN: 2381-7496 (Online)

Security Issues, Threats and Possible Solutions in Cloud Computing

Emmanuel Kolawole*, Warsame Ali, Olusegun Odejide, John Fuller

Department of Electrical and Computer Engineering, Prairie View A&M University, Prairie View, USA

Abstract

In today's advancement, Information Technology infrastructure continues to grow with the evolution of daily technology. The invention of the Internet has increased the use of computer and the mobile device. Nowadays, many people in the world use these devices, and as a result, a large amount of data stored device and each device in the Internet were required to be connected to each other because of sharing information. This innovation then brought about Cloud computing which is an Internet-based computing where shared resources, software and information are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. This paper shows Successful implementation of cloud computing in an enterprise which requires proper planning and understanding of emerging risks, threats and possible countermeasures. This paper also shows how we secure the cloud security, privacy and reliability when a third party is processing sensitive data. In this paper, we have discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. This paper also covers the advantages and disadvantages of cloud computing. Finally, this paper identifies security threats focused on cloud computing which is an essential part of the companies that want to use cloud computing services, and some solutions about security threats for enterprise and service provider for the cloud computing deployment to provide the security of information.

Keywords

Cloud Computing, Enterprise Computing, Risk, IaaS, PaaS, SaaS, Security, Threats, Controls, CIA

Received: March 1, 2019 / Accepted: April 8, 2019 / Published online: May 5, 2019

1. Introduction

Cloud computing is the most trending technology among IT sector because of its characteristics like rapid elasticity, broad network access, measured services, on-demand self-service and resource pooling [1]. It involves delivering computing resources (hardware and software) as a service over a network (typically the internet) by cloud computing service providers.

Nowadays, the Internet continues to grow, and greater amount of information is being transferred. Adding smart phones and tablet pc's to this environment. As a result, data and application in Internet and mobile have continuously increased [2]. All these technological developments provide new business model which is cloud computing. Cloud computing is an important solution and cost-effective model to facilitate companies' computing needs and accomplish business objectives [2, 3].

The figures 1, 2, and 3 below show different examples of a Cloud Computing environment.

* Corresponding author
E-mail address: ekolawole@student.pvamu.edu (E. Kolawole)

Figure 1. Cloud Computing [4].

Figure 2. Cloud Computing [5].

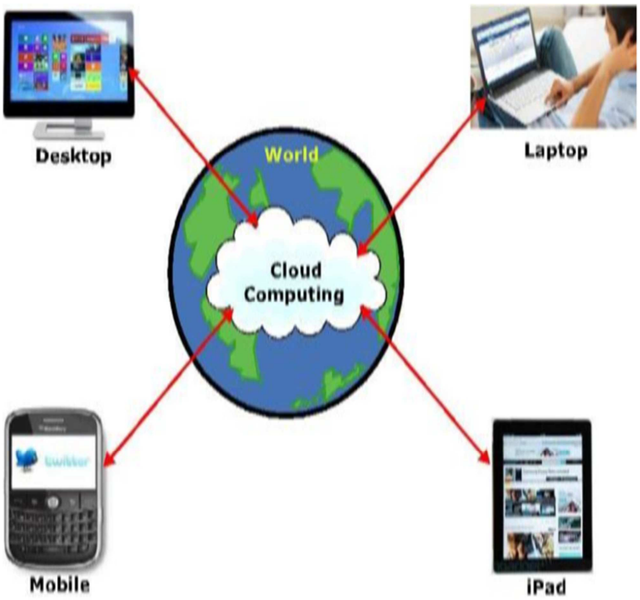


Figure 3. Cloud Computing [6].

2. Cloud Service Models

Cloud service models describe how cloud services are made available to clients. Most fundamental service models include a combination of System layer called IaaS (Infrastructure as a service), the Platform layer called PaaS (Platform as a service), and the Application layer called SaaS (software as a service) [5]. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[a] System Layer- Infrastructure as a Service (IaaS)

This is the lowest-level cloud service paradigm and the most important. The model provides infrastructure components to clients. With IaaS, pre-configured hardware resources are provided to users through a virtual interface [11]. Unlike PaaS and SaaS, IaaS does not include applications or even an operating system (implementation all of that is left up to the customer) [3]. In other word, it provides services to the companies with computing resources including servers, networking, storage and data Centre space on a pay-per-use basis. The capacity provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). With IaaS, clients have direct access to the lowest-level software in the stack; that is, to the operating system on virtual machines, or to the management dashboard of a firewall or load balancer. Amazon Web Services is one of largest IaaS providers. It simply enables access to the infrastructure needed to power or support that software. IaaS can provide extra storage for corporate data backups, network bandwidth for a company which was previously only accessible to those with supercomputers. Popular IaaS offerings like Amazon EC2, IBM SoftLayer, and Google's Compute Engine (GCE) are silently powering a huge portion of the backbone of the internet, whether users realize it or not.

[b] Platform Layer- Platform as a Service (PaaS)

PaaS is a cloud service model where the cloud is used to deliver a platform to users from which they can develop, initialize and manage Applications [11]. In this model, you can use Web-based tools to develop applications, so they run on systems software which is provided by another company, like Google App Engine. The model delivers a pre-built application platform to the client; clients needn't spend time building underlying infrastructure for their applications. PaaS offerings typically include a base operating system and a suite of applications and development tools. PaaS eliminates the need for organizations to build and maintain the infrastructure traditionally used to develop applications [3]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Popular PaaS products are Google's App Engine, IBM BlueMix, and Apache's Stratos which are helping to streamline and democratize software development. Figures 4, 5 and 6 show the typical layers of cloud computing.

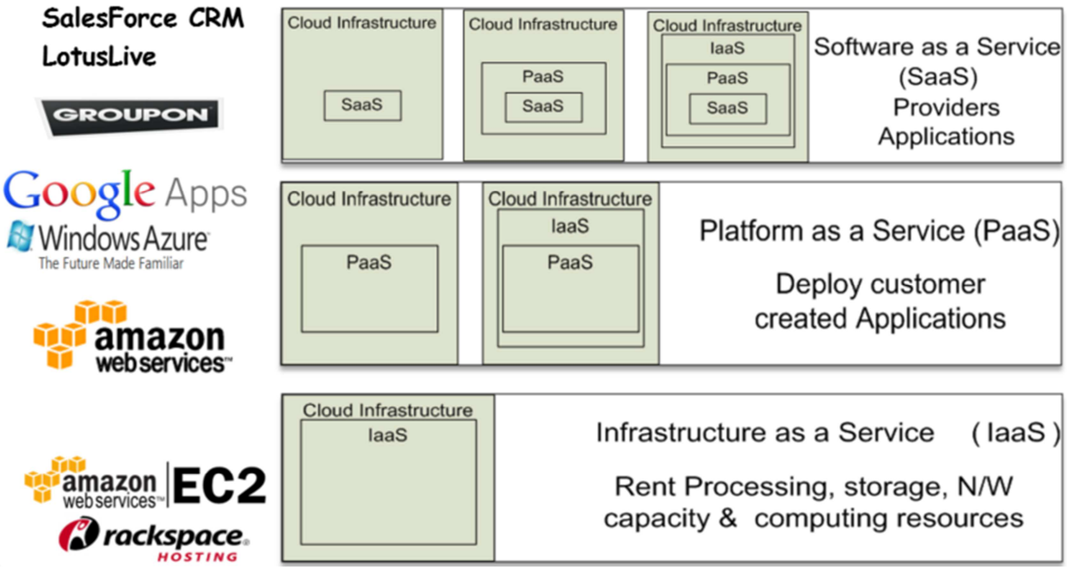


Figure 4. Layers of Cloud Computing [4].

[c] Application Layer- Software as a Service (SaaS)

This is sometimes referred to as on-demand software. SaaS is a software licensing and delivery model where a fully functional and complete software product is delivered to users over the web on a subscription basis [11]. It is also called a delivery model where the software and the data which is associated with is hosted over the cloud environment by third party is called cloud service provider, like your Gmail account, you use that application on someone else's system. SaaS offerings are typically accessed by ends users through a web browser (making the user's operating system largely irrelevant) and can be billed based on consumption or with a flat monthly charge. The SaaS software provider has complete control of application software. As known SaaS offerings are the most widely visible of all the cloud computing service models. In most cases, many users are using SaaS products without even realizing it. The capacity provided to the consumer is to use the producer's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface [3]. The consumer does not manage or control the systems, storage, or even individual application capabilities, but, there is possible exception of limited user-specific application configuration settings. SaaS application examples include online mail, project-management systems, CRMs, and social media platforms. Popular products like Office 365 and Salesforce have thrust SaaS offerings to the forefront of the workplace and are used by thousands of businesses on daily basis.

"IaaS"
Infrastructure-as-a-Service
host
"PaaS"
Platform-as-a-Service
build
"SaaS"
Software-as-a-Service
consume

Figure 5. Layers of Cloud Computing [3].

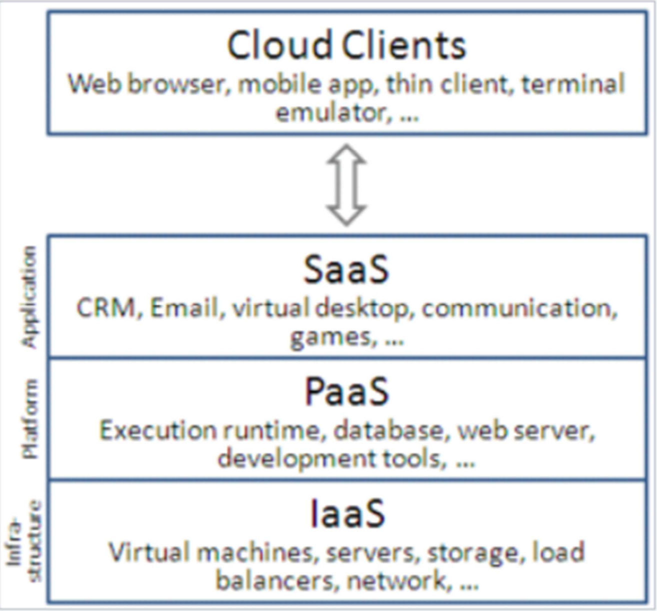

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Figure 6. Cloud Computing [6].

3. Cloud Security Attacks for Cloud Based Computing

The cloud had opened a whole new frontier for storage, access, flexibility, and productivity which has enhanced a new world of security concerns. SaaS, PaaS and IaaS also disclose information security issues and risks of cloud computing systems. Thou Cloud computing might be seen as a remedial solution to all problems but despite its advantages, there are several considerable drawbacks that should be taken into consideration [11]. Transferring enterprise IT to the cloud is a complex task that includes both technical and organizational challenges. The cloud is a new paradigm that doesn't have a clear sentence definition; it includes multiple factors, and therefore transformation to a cloud-based process may seem confusing. This complexity paired with uncertainty creates a number of organizational cloud-adoption barriers. Below are some top Security Concerns for Cloud-Based Services.

[a] Data Breaches-Cloud computing and services are relatively new, yet data breaches in all forms have existed for years [3]. The question remains; "with sensitive data being stored online rather than on premise, is the cloud inherently less safe?" A study conducted by the Ponemon Institute entitled "Man In Cloud Attack" reports that over 50 percent of the IT and security professionals surveyed believed their organization's security measures to protect data on cloud services are low. This study used nine scenarios, where a data breach had occurred, to determine if that belief was founded in fact. After evaluating each scenario, the report concluded that overall data breaching was three times more likely to occur for businesses that utilize the cloud than those that don't. The simple conclusion is that the cloud comes with a unique set of characteristics that make it more vulnerable. Data breach can also be defined as the leakage of sensitive customers' or organizations' data to unauthorized users. In the same scenario, data breach from organization can have a very huge impact on its business regarding finance, trust, loss of customers as well as loss of intellectual properties. This may happen accidently due to flaws in infrastructure, software, application designing, operational issues, insufficiency of authentication, authorization, and audit controls [15].

[b] Hijacking of Accounts-The growth and implementation of the cloud in many organizations has opened a whole new set of issues in account hijacking. Attackers now can use your (or your employees') login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials [3]. Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [10]. Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials. In April 2010 Amazon faced a cross-site scripting bug that targeted customer credentials as well. Phishing, keylogging, and buffer overflow all present similar threats. However, the most notable new threat – known as the Man In Cloud Attack – involves the theft of user tokens which cloud platforms use to verify individual devices without requiring logins during each update and sync. In this same scenario, a clickjacking attack generally is considered an adversarial activity at the transport layer [12]. This type of attack is usually attached to a browser, in which the attack is launched by a clickable object on the page with embedded adversarial codes or a script. Wu et al. [13] emphasized a stealthy clickjacking attack could take place by clicking on any malicious object on the page; this can be in a case of a fake system reminder. Users would not notice the dubious activities since relaunching malicious software could be automatic, such as using a timer. Some examples of clickjacking included Likejacking [14] and Cursorjacking.

[c] Insider Threat- An attack from inside your organization may seem unlikely, but the insider threat does exist [3]. Employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information [10]. Additionally, these insiders don't even need to have malicious intentions. A study by Imperva, "Inside Track on Insider Threats" found that an insider threat was the misuse of information through malicious intent, accidents or malware. The study also examined four best practices companies could follow to implement a secure strategy, such as business partnerships, prioritizing initiatives, controlling access, and implementing technology.

[d] Malware Injection- Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves [3]. Hackers exploit vulnerabilities of a web application and embed malicious codes into it changing the course of its normal execution. The two common forms are SQL injection attack and cross-site scripting attack. Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data. Security Threats on the said Cloud Computing Vulnerabilities, a report by the East Carolina University, reviews the threats of malware injections on cloud computing and states that "malware injection attack has become a major security concern in cloud computing systems." Figures 7 & 8 shows the typical representation of a

Malware injections and Cross-site scripting attacks.

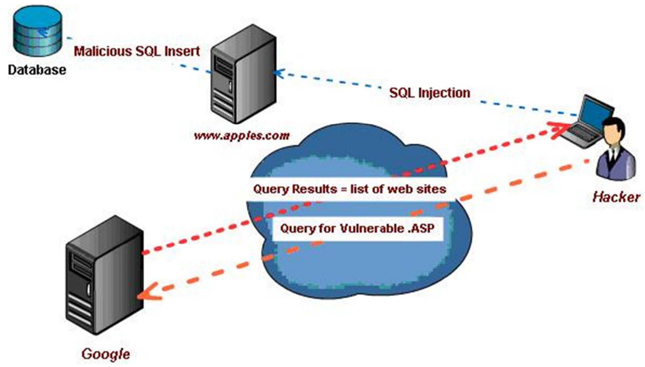
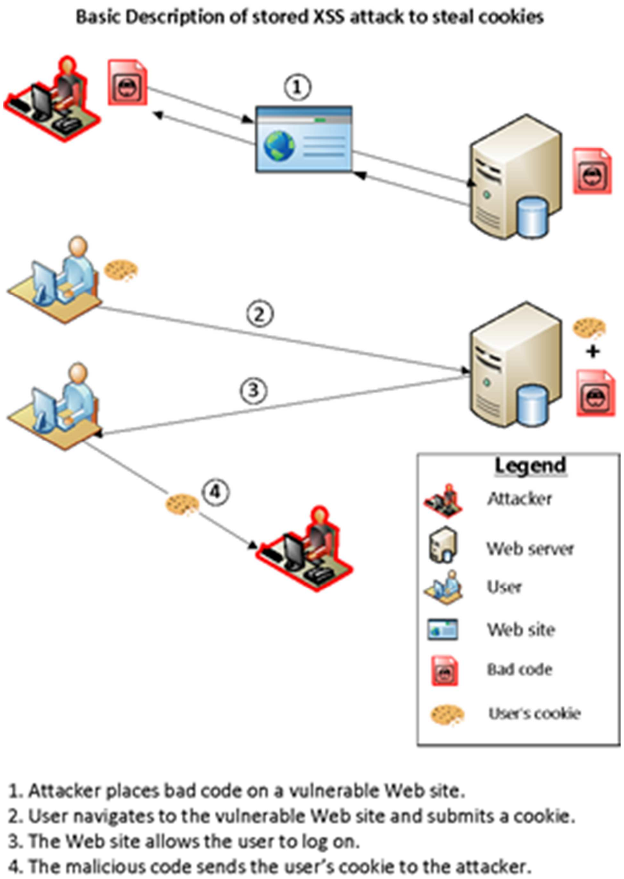


Figure 7. Malware injection attacks [4].



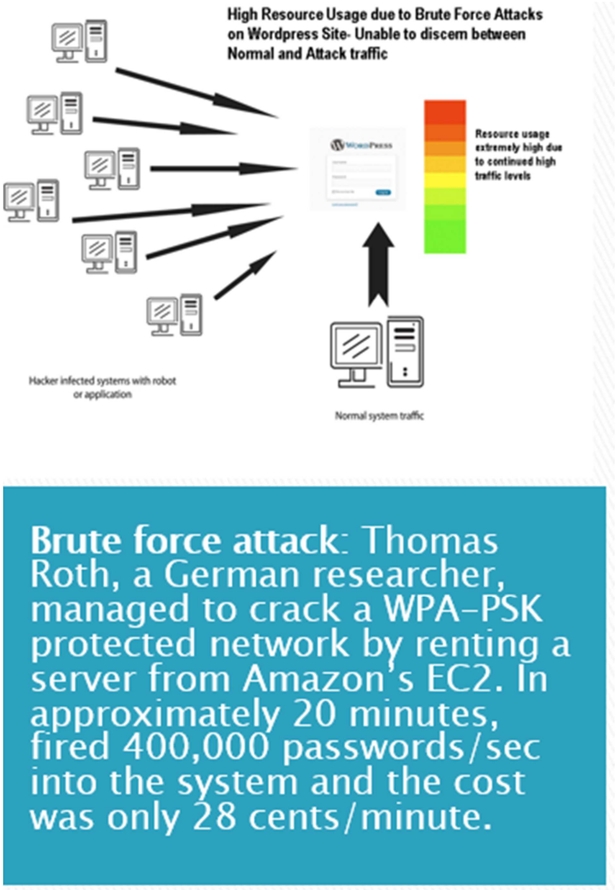
1. Attacker places bad code on a vulnerable Web site.
2. User navigates to the vulnerable Web site and submits a cookie.
3. The Web site allows the user to log on.
4. The malicious code sends the user's cookie to the attacker.

Figure 8. Cross-site scripting attacks [4].

[e] Multi-tenancy: Is a major concern in cloud computing. Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server.

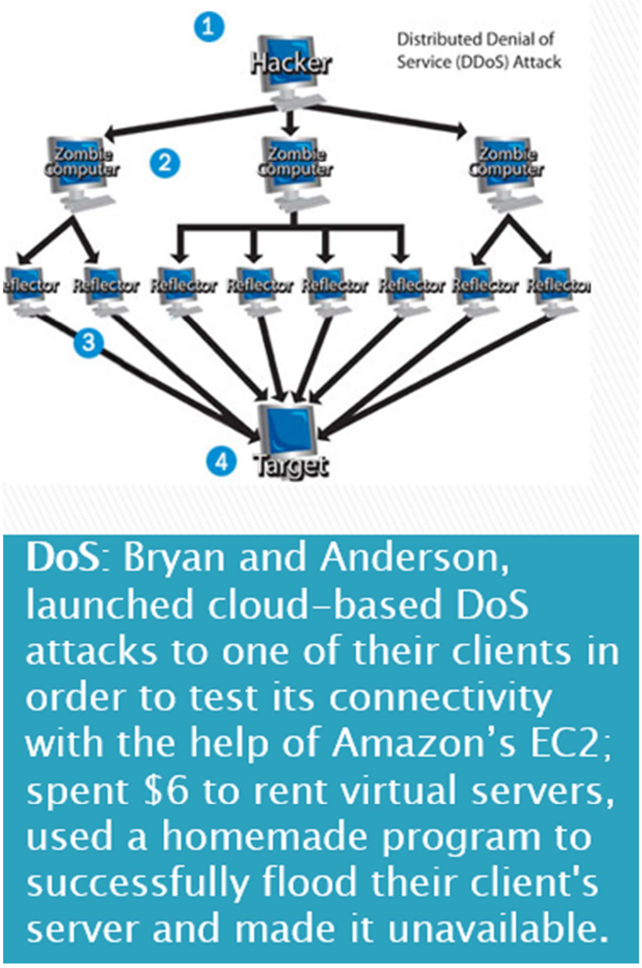
Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server [10].

[f] Abuse of Cloud Services- The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily [3]. Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking or password [10]. However, with the level of the cloud's unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties. In some cases, this practice affects both the cloud service provider and its client. For example, privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider [4]. These risks include the sharing of pirated software, videos, music, or books, and can result in legal consequences in the forms of fines and settlements with the U.S. Copyright Law reaching up to $250,000. Depending on the damage, these fines can be even more cost prohibitive. Previously, hackers used multiple computers or a botnet to produce a great amount of computing power in order to conduct cyber-attacks. Today, powerful computing infrastructure could be easily created using a simple registration process in a cloud computing service provider. This resulted in Brute force attack and Denial of Service attack as shown in figures 9 and 10 below.


High Resource Usage due to Brute Force Attacks on Wordpress Site- Unable to discern between Normal and Attack traffic
WordPress
Resource usage extremely high due to continued high traffic levels
Hacker infected systems with robot or application
Normal system traffic

Brute force attack: Thomas Roth, a German researcher, managed to crack a WPA-PSK protected network by renting a server from Amazon's EC2. In approximately 20 minutes, fired 400,000 passwords/sec into the system and the cost was only 28 cents/minute.

Figure 9. Brute force attack [4].



DoS: Bryan and Anderson, launched cloud-based DoS attacks to one of their clients in order to test its connectivity with the help of Amazon's EC2; spent $6 to rent virtual servers, used a homemade program to successfully flood their client's server and made it unavailable.

Figure 10. Denial of Service attack [4].

[g] Insecure API- Application Programming Interfaces (API) give users the opportunity to customize their cloud experience. However, APIs can be a threat to cloud security because of their very nature. Not only do they give companies the ability to customize features of their cloud services to fit business needs, but they also authenticate, provide access, and effect encryption [3]. Customers handle and interact with cloud services through interfaces or API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks [10]. As the infrastructure of APIs grows to provide better service, so do its security risks. APIs give programmers the tools to build their programs to integrate their applications with other job-critical software. A popular and simple example of an API is YouTube where developers can integrate YouTube videos into their sites or applications. The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks.

[h] Denial of Service Attacks- Unlike other kind of cyberattacks, which are typically launched to establish a long-term foothold and hijack sensitive information, denial of service assaults do not attempt to breach your security perimeter [3]. Rather, they attempt to make your website and servers unavailable to legitimate users. In some cases, however, DoS is also used as a smokescreen for other malicious activities, and to take down security appliances such as web application firewalls [4].

[i] Insufficient Due diligence- Most of the issues we've looked at here are technical in nature, however this security gap occurs when an organization does not have a clear plan for its goals, resources, and policies for the cloud [3]. In other words, it's the people factor. Additionally, insufficient due diligence can pose a security risk when an organization migrates to the cloud quickly without properly anticipating that the services will not match customer's expectation. This is especially important to company whose data falls under regulatory laws like PII, PCI, PHI, and FERPA or those that handle financial data for customers.

[j] Shared Vulnerabilities- Cloud security is a shared responsibility between the provider and the client. This partnership between client and provider requires the client to take preventative actions to protect their data [3]. While major providers like Box, Dropbox, Microsoft, and Google do have standardized procedures to secure their side, fine grain control is up to you, the client. As Skyfence points out in its article "Office 365 Security & Share Responsibility," this leaves key security protocols – such as the protection of user passwords, access restrictions to both files and devices, and multi-factor authentication – firmly in your hands. The bottom line is that clients and providers have shared responsibilities and omitting yours can result in your data being compromised.

[k] Data Loss- Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider [3]. Losing vital information can be devastating to businesses that don't have a recovery plan. Comprised data may include; deleted or altered data without making a backup; unlinking a record from a larger environment; loss of an encoding key; and illegal access of sensitive data [10]. Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers' data in 2011. Google was another organization that lost data when its power grid was struck by lightning four times. Securing your data means carefully reviewing your provider's back up procedures as they relate to physical storage locations, physical access, and physical disasters.

[l] Multi-tenancy: Is a major concern in cloud computing. Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server. Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same

data-storage system and both the attacker and the sufferer are sharing the common server [10].

[m] Network attacks: Presently, it is obvious that network attack is still the biggest challenge of network security due to the verse diversity of newer technologies in the industries [16]. As more and more packages, applications, customers, and enterprises migrate their data into the cloud computing environment, cloud computing will appear to be more prone to network attacks and fraud. Recent release from security experts concluded that cloud computing will be the focus of hackers within five years.

4. Solution to Security Issues in Cloud Based Computing

In today's technology, there are several types of security threats to which cloud computing is vulnerable. These threats damage confidentiality, integrity and availability (CIA) security model. Accordingly, solutions of security threats aim to protect CIA security model. In this paper, we will discuss some measures in addressing the security threats to cloud computing.

[a] Find Key Cloud Provider- Cloud computers' customers must find the best cloud provider. Each cloud service provider has different data security and data management [7]. Hence, customer determines requirements for cloud services then choose the right provider. Also, cloud provider must have experience, standards and regulation about cloud service.

[b] Secured Data Transfer- Since data transfer between customers' network and cloud on the internet, therefore, data must be always travelling on a secure channel. HTTP is insecure due to data been sent in a plain text. Attackers gain access to website accounts and sensitive information with man-in-the-middle and eavesdropping attacks. Connect to browser with HTTPS because everything in the HTTPS message is encrypted with SSL. Also, protocols should be used as well for authentication [8].

[c] Access management- User access control is important in cloud computer because of sensitive and private data. Only authorized persons should see the information and persons should be authorized they need it. Customers to ask service providers for specific questions about the people who manage their data and the level of access they have to it [9]. Because data for multiple customers may be co-located in cloud, other people may be able to access other customers' data. It is an important risk for sensitive data. Cloud service vendors must provide best access management for cloud customers. Continuous monitoring of physical computing systems, restricting traffic access to the data using firewalls, IDS and controlling access to cloud applications and data using SAML and XACML. [4]

[d] Auditing- All systems and network components log must be stored and monitored to analyze unwanted events. Logging and monitoring events is the process of auditing. Auditing is important for analyzing events. Auditing is necessary to provide security [9]. Cloud computing customers discuss cloud provider about monitoring logs day-to-day. In addition, the audit log should be centrally preservers. Authentication and authorization should be done for people to monitor the audit log.

[e] Security Testing-This is important to provide security in cloud computing. Security tests should be performed for software before deployment in infrastructure of cloud. Software patches should be tested for security before software patches to install. Additionally, security testing should be realized continuously to identify vulnerabilities in the cloud system [9]. On the risk assessment, some of these tests may be performed by third parties. There should also be a process to resolve identified vulnerabilities.

[f] System Synchronization- If all systems in the data center are synchronized to the same clock, this is helpful both to ensure correct operation of the systems, as well as to facilitate later analysis of system logs [9]. If time zone is different, it is big problem for logs and synchronizes systems. Data has needed to analyze the event such as the time when a problem about security-related events.

[g] Data Encryption-In a cloud, with shared storage, encryption is a key technology to ensure isolation of access [9]. The cloud infrastructure needs to provide secure facilities for the generation, assignment, revocation, and archiving of keys. It is also necessary to generate procedures for recovering from compromised keys.

[h] Policy and Standardization- Policies, standards and guidelines should be developed, documented, and implemented. Cloud computing providers must be up to these standards and policies [9]. To maintain relevancy, these policies, standards, and guidelines should be reviewed at regular intervals or when significant changes occur in the business or IT environment.

[i] Security Techniques Implementation- For malware injection attacks, use FAT system; also store a hash value on the original service instance's image file and perform integrity check. For XML signature wrapping attacks, use XML Schema Hardening techniques i.e. a subset of XPath, called FastXPath [4].

[j] Data Protection-Data loss prevention systems, anomalous behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization. Cloud provider may

improve process that including a cloud-wide intrusion and anomaly detection system. The intrusion detection systems may be installed an infrastructure for security [4].

[k] Security Policy Enhancement-Avoid weak registration systems, credit card fraud monitoring, and block of public black lists could be also applied [4].

[l] Training- Trainings or programs should be developed that provide a baseline for providing fundamental security and risk management skills and knowledge to the cloud computing providers, the security team and their internal partners [9].

5. Conclusions

Cloud Computing is in continual development while people enjoy the benefits that cloud computing brings. It is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises, but the security risk is also enormous. Organizations looking into cloud computing technology to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. Although cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is also much to be cautious about with respect to its security. With the advent of newer technologies in the industries on daily basis, cloud computing has become an important computing paradigm and has been dominating the IT market the more. Based on this evaluation, more shift towards cloud computing can be seen in the future because of its features and benefits. With this revolutionization of computing world by cloud, it is prone to number of security challenges as well which may vary from application to network level in which the security risks must be controlled. Even the data residing inside the cloud is vulnerable to attacks. Much vulnerability in clouds still exists and hackers continue to exploit these security holes. In this paper, we have examined the security vulnerabilities in clouds and included related real-world exploits and introduced the countermeasures to those security breaches.

In the future, further efforts in studying cloud security risks and the countermeasures to cloud security breaches must continue. In this effort, we are investigating in the cloud security management problem. Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. Since security is a major threat to the cloud computing because the data placed on cloud servers is always vulnerable as there are lots of attackers on the internet who tries to compromise the security of the cloud. To overcome this issue, we will investigate the use of security appliances in the form of physical machines or by virtualization. A significant amount of power is consumed by security appliances which not only leads to the high energy costs but also a major threat to the environment as carbon-dioxide is released. So, there is a need to find optimal solutions for providing security in cloud computing environment in an efficient manner. In our future work, a new framework will be proposed to provide security in virtual networks that is based on Intrusion Detection and Prevention System (IDPS).

References

[1] NIST, “The NIST definition of cloud computing”, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf. Accessed on 12 Aug, 2015.

[2] http://www.ece.rutgers.edu/~psannuti/ece224/PEEII-Expt-2-07.

[3] https://www.incapsula.com/blog/top-10-cloud-security-concerns.html

[4] Te-Shun Chou, “Security Threats on Cloud Computing Vulnerabilities,” International Journal of Computer Science & Information Technology (IJCSIT) Vol. 5, No 3, June 2013.

[5] J. Stirling, “HP unveils more public loud service info”, http://www.itpro.co.uk/639508/hp-unveils-more-public-cloudservice-info. 12.3.2012.

[6] http://en.wikipedia.org/wiki/Cloud_computing

[7] Pradeep Kumar Tiwari, Dr. Bharat Mishra “Cloud Computing Security Issues, Challenges and Solution.” International Journal of Emerging Technology and Advanced Engineering. (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[8] N. Brender, I. Markov, "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies", International Journal of Information Management 33 (2013) 726-733.

[9] Hanim Eken, Gazi University, Ankara, Turkey, “Security Threats and Solutions in Cloud Computing” World Congress on Internet Security (WorldCIS-2013). 978-1-908320-22/3/2013 IEEE.

[10] Kashif M and Prof Dr. Sellapan P, “Framework for Secure Cloud Computing International Journal on Cloud Computing” Services and Architecture, (IJCCSA), Vol. 3, No. 2, April 2013.

[11] Sophia Palmira, Saas, PaaS, and IaaS: Understanding the Three Cloud Computing Service Models https://doublehorn.com/saas-paas-and-paas-and-iaas, https://doublehorn.com/saas-paas-and-iaas-understanding. August 24, 2017.

[12] Xiaotong Sun, " Critical Security Issues in Cloud Computing: A Survey ", IEEE International Conference on Big Data Security on Cloud, pages 216-221, New York, NY, USA, 2018.

[13] L. Wu, B. Brandt, X. Du, and B. Ji. “Analysis of clickjacking attacks and an effective defense scheme for android devices” Communications and Network Security (CNS), 2016 IEEE Conference on, pages 55–63, Philadelphia, PA, USA, 2016.

[14] Muhammad Kazim, “A survey on top security threats in cloud computing” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015.

[15] C. S. Alliance, “Top threats to cloud computing v1. 0,” Cloud Security, Alliance, USA, 2010.

[16] Wag Jun-jie, Mu Sen, "Security Issues and Countermeasures in Cloud Computing ", IEEE International Conference, pages 843-846, Nanjing, China, 2011.