Cloud computing and security challenge

Zolkipli, Mohamad Fadli
School of Computing
Universiti Utara Malaysia
Kedah, Malaysia
m.fadli.zolkipli@uum.edu.my

Riduan, Azrin Iman
School of Computing
Universiti Utara Malaysia
Kedah, Malaysia
imanazrin12@gmail.com

***Abstract*— Cloud computing is a network-based technology that provides computation, information, data, and storage services. For effective product growth, the software industry is placing a greater focus on Quality Assurance (QA) and Testing criteria. Presently. Testing is an effective way to identify potential vulnerabilities before real-world situations arise to ensure a high degree of protection for cloud services and applications. As a result, several public cloud providers announced that businesses are increasingly encouraging Testing Centers of Excellence (COE) and software test automation. This paper examines cloud protection testing from a crucial standpoint. Gaps in recent related journals, testing tools, and software test automation deals are also exposed. The potential research implications are highlighted to improve understanding and relationships between current research fields. The cloud infrastructure paradigm has transformed the computing world as it offers improved reliability, vast scalability, and reduced costs have drawn both companies and individuals. It adds information systems capability.**

Keywords*— *Cloud computing, cloud testing, security, vulnerability

I. Introduction

Cloud computing is a trendy and state-of-the-art IT sector solution. Organizations, in particular, benefit from cloud computing's unique advantages, such as improved scalability and portability, which result in increased efficiency and cost savings. Research on the identification of challenges and benefits of cloud computing has been done since 2008[1]. Applications are hosted, deployed, and delivered over the Internet in cloud computing. Cloud applications can adapt to their highly secure and reliable environmental changes. Power, storage, and virtualization are the infrastructure on which cloud applications are built. Cloud Computing Security Lab focuses on cloud testing software and seeks to develop new approaches, tools, and techniques to enhance the testability of cloud-based applications. The cloud computing allows the program framework to work for these internet-enabled computers. This hosting platforms are generally divided into three different categories: IaaS, PAAS, software-as-a-service and IaaS. (SaaS). Customers use a cloud platform when and when required, normally on an annual rate. Other advantages of cloud computing are scalability and increased flexibility for a relatively constant price. [2]. Any of the fundamental security risks abused the use of cloud computing. Botnets, the usage of botnets to distribute spam and malware are an example of a security problem. Among the 761 privacy violations prosecuted by the U.S. Secret Service in 2010 nearly 63% happened in businesses with 100 or less workers. And a study conducted by Technology Company Symantec Corp. in 2011 showed that about 2000 plus small and medium-size companies had violated almost 73% of cyber-attacks.

II. CLOUD COMPUTING MODELS

Cloud hosting deployment models are classified by ownership, size, and access. It tells of the nature of the cloud. Most organizations, because they reduce transaction costs and controls, are ready to implement the cloud. Many Companies that are considered to be giants in software industry like Microsoft are joining to develop Cloud services [3]

- Public Cloud

There would be very little to no distinction between public and private cloud structures but for the degree of protection that cloud storage companies get through different cloud infrastructure providers' systems. Cloud service is appropriate for companies requiring load control. Because of reduced capital overhead and operating costs, the public cloud paradigm is economical. Dealers can have a free service or license policy including pay per consumer. Both public cloud customers bear the bill. It supports consumers by economies of scale. Free online cloud providers may be accessed, e.g., Google is a public cloud.

- Cloud Computing in the Private Sector

It is also known as an internal cloud. This cloud storage infrastructure is designed into a stable cloud system and secured by a firewall that is run by a specific company's IT department. The private cloud only enables registered customers to access their data and increases the organization's control. The actual machines may be hosted internally or externally and are equipped with capital from another pool. Unpredicted or complex companies choose to take on a private cloud of functions that are essential maintenance needs and uptime requirements. In private cloud, there should be no extra protection regulations and bandwidth limits in a public cloud setting. As device access and networks are limited, the technology is managed and improved by consumers including cloud service providers. One of its strongest instances were Eucalyptus Systems.[4]

- Hybrid Cloud

It was a kind of cloud storage that is embedded. It may be a blend of two or more cloud servers, such as a private, public, or group cloud which is connected together and separate. Hybrid clouds are unable to be categorized as public, private, or group clouds because they can transcend isolation and circumvent supplier limitations. By assimilation, aggregation, and personalization, it allows the customer to maximize the availability and capacity of a particular cloud package service. The services in a hybrid cloud are either handled by external providers or handled internally. It is a cross-platform adaptation in which workloads are moved between the private cloud and the public cloud based on corporate demand and requirements. Non-critical tools, such as creation and research workloads, may be hosted on a third-party service provider public cloud. They can be housed internally during vital or sensitive workloads. The hybrid cloud architecture for Big Data can be used by businesses. Scalability, flexibility, and reliability are some of the benefits of hybrid cloud hosting.

- Community Cloud

It is a kind of cloud hosting in which many organizations, such as banks and trading companies, share the set-up. It is a multi-tenant organization shared between a few organizations in a community that have common machine fears. Those in the neighborhood are generally concerned with the same things when it comes to success and protection. Internally, publicly, or internally by third-party vendors, the community cloud may be handled. The community cloud saves money when the expenses are borne by many organizations in the community. Organizations have discovered that cloud hosting has a lot of promise. To be the greatest, you must choose the appropriate cloud storage service. As a result, it is essential to have a thorough understanding of the business and its requirements. It is simple to accomplish business objectives until the right cloud computing type is chosen.

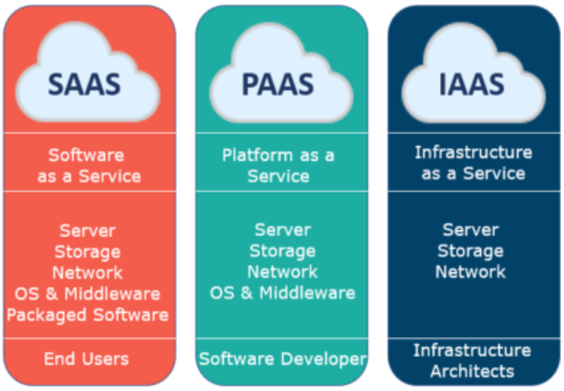

Fig. 1. Model of Cloud Infrastructure Service

- Software as a Service (SaaS)

SaaS is a model that provides quick access to cloud-based web applications. Software as a service. The seller controls the entire computer stack, which can be accessed via a web browser. These applications run on the cloud and can be used with a paid, license subscription or with limited access free of charge. The cloud provider provides the consumer with the ability to deploy an application on a cloud infrastructure [5]. SaaS would not enable you to install or import something into the current computing system. Which removes the need for the supplier's servicing and assistance to update software on each unit. Google G Suite, Microsoft Office 365, Dropbox, as well as well SaaS examples are only a few examples. As shown in Fig. 1, models of cloud infrastructure services.[6]

- Platform as a Service (PaaS)

Platform as a Service or PaaS is essentially a cloud base to create, evaluate and organize the different business applications. Implementing PaaS simplifies the application development creation phase. PaaS offers a simulated runtime environment for application development and training. Either that the business or a cloud vendor may handle the whole infrastructure of servers, storage, and networking. Two typical examples of PaaS are Google App Engine and AWS Elastic Beanstalk. PaaS also provides subscription-based pricing options for you depending on your business requirements.

- Infrastructure as a Service (IaaS)

IaaS or Service Infrastructure is basically a virtual supply of cloud computing resources. An IaaS cloud supplier can provide you with a wide range of computer infrastructures, including storage, servers, maintenance, and support for networking hardware. Companies can choose to compute resources without installing hardware on their premises. Some of the leading IaaS cloud service providers are Amazon Web Services, Microsoft Azure and Google Compute Engine.

III. SECURITY ISSUES

Consumers may use cloud infrastructure models to access a wide range of services. IaaS is on the bottom layer, providing directly with the strongest features of the entire cloud. IaaS allows hackers to carry out attacks, such as brute cracking, which require high computer capacity. IaaS allows for the creation of several virtual devices, making it an excellent forum for hackers to execute attacks that involve a diverse set of skills. Another vulnerability issue associated with cloud models is data leakage.

Data in cloud models is easily accessible by unauthorized internal employees and external hackers. Internal employees may quickly gain access to records, either deliberately or unintentionally. External hackers can access databases in these settings by using hacking techniques such as hijacking and eavesdropping on the network channel. Virus and Trojan may be loaded into the cloud and damaged [7].

- Compromised credentials and broken authentication

When they want to issue approvals that are suitable for the user's position, organizations and businesses often have issues with identity management. While switching job functions or leaving the business, it is common to neglect and delete user access. Because of stolen account accounts, Anthem's data theft compromised more than 80 million consumer information. Anthem had not implemented multifactor authentication. Therefore, when the attackers got the credentials, everything was over. Many developers have mistaken to incorporate credentials and encryption keys into their source code and have them in publicly available repositories [8].

- Data breaches

Cloud systems pose all the same threats as conventional enterprise networks, but cloud services have become appealing because cloud servers hold a vast volume of data. The severity of the exposure is usually determined by the sensitivity of the data that has been exposed. The title goes to personal records, but breaches of government information and trade secrets may be much more damaging. An organization could face legal consequences if there is a cyberattack. Investigations into infringement and consumer alerts may be costly. Indirect impacts may entail reputation degradation and market failure, which may have long-term consequences for potential organizations.

- Hacked interfaces and APIs

APIs are also eligible for any cloud provider and programmed widely available. These frameworks and APIs are used by IT departments to handle and communicate to cloud systems such as cloud service providers, cloud administration, and tracking services. The API's protection is what determines the cloud's reliability and data. Third parties that depend on and expand on APIs put themselves at risk because businesses can need further expertise and certificates to be exposed. APIs and weak interfaces may expose organizations, such as confidentiality, accountability, accessibility to security concerns the highly exposed part of the system is its APIs and interfaces, since it can be accessed over the open Internet [9].

- Exploited system vulnerabilities

System vulnerabilities and exploitable programmed bugs have become a bigger problem in cloud computing with the advent of multi-tenancy. In close proximity, organizations share memory, databases, and resources, creating new attack surfaces. Device vulnerability mitigation costs are comparatively modest as compared to other IT expenses. The expense of applying IT processes to detect and patch exploits is insignificant when compared to the possible risk.

- Account hijacking

Phishing, spam, and malware vulnerabilities are all very common these days, and the vulnerability is also being extended to cloud providers so offenders can listen in on conversations, control purchases, and change records. Intruders may be using the database framework to carry out additional assaults. Institutions must preclude the exchange of customer and service account credentials and, when possible, implement multifactor authentication schemes. Each transaction must be traced back to a human user, so accounts must be closely watched. The key is to keep account credentials from being compromised [10].

- Permanent data loss

Hackers have previously taken data to damage businesses from cloud data centers, and cloud data centers are much like all other facilities susceptible to natural disasters. For better security, cloud providers can require that apps and data be spread through several zones. The importance of proper data backup and disaster recovery procedures cannot be overstated. The importance of regular data backup and off-site storage while using the cloud cannot be overstated. Data failure prevention is the responsibility of both the cloud storage company and the data provider. The user will encrypt the data before uploading to the cloud however, the authentication key must be held safe. If the key is absent, the data is also lost. Compliance procedures also dictate how long audit logs and other paperwork must be maintained by organizations. The loss of such classified details may have serious implications.

- Inadequate diligence

Without a thorough knowledge of the landscape and the challenges associated, cloud infrastructure firms may be exposed to a wide range of corporate, financial, technological, regulatory, and enforcement risks. If the enterprise seeks to transition to the cloud or combine with another cloud provider, caution is needed. Institutions who refuse to check the deal, for example, might not be mindful of the supplier's liability in the case of data failure or violation. When applications are deployed for a specific cloud, operational and architectural issues may occur if the cloud systems are unfamiliar to the organization's developer. Because of the dangers associated with cloud computing, a company should perform proper analysis before making the switch [11].

- Abuse of cloud service

Cloud services may be used to enable operations such as breaking an encryption key and launching an assault using cloud storage. DDoS assaults, junk mail, and phishing are examples of these types of attacks. Clients need resources to track the health of their cloud systems, and providers need to understand how DDoS attacks are being used. Customers can check to see if their service company has a system for disclosing harassment. Despite the fact that consumers are not actively subjected to malicious activity, cloud service misuse can result in a loss of service and knowledge [12].

- DoS attacks

DoS assaults have been overdue for a long time and have resurfaced in recent years as a result of cloud infrastructure, where they often disrupt accessibility. Systems may run slowly or only for a short period of time. These DoS attacks use a lot of computing resources, which the user would eventually have to pay for. While high-volume DDoS attacks are normal, organizations should be aware of asymmetrical and application-level DDoS attacks that threaten web servers and databases. DoS attacks are more common among cloud vendors than among their clients. The key is to have a strategy in place before the assault to minimize the damage and ensure that administrators have access to the tools they need. The following table depicts the process of a DoS strike. Fig. 2 shows the process of DoS strike.[13]

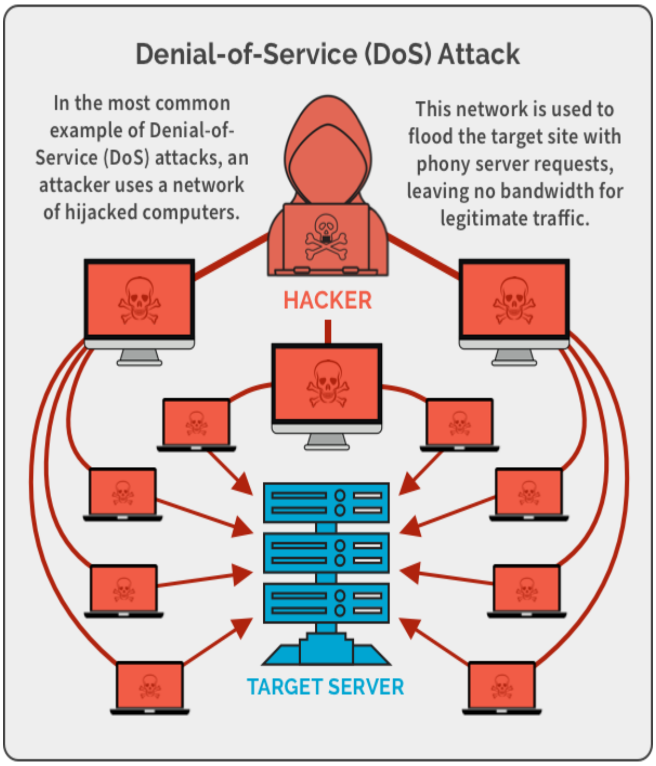
Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

Fig. 2. Denial-of-Service (DoS) Attack

IV. SECURITY CHALLENGES OF CLOUD MODEL

- Malicious attacks

There can be security threats both from outside and within organisations. According to the Cyber Security Watch Survey 2011, an insider account for 21% of cyber-attacks. 33% of respondents felt that the insider attacks were more costly and harmful to organisations. Insider assaults were also used to gain unauthorised access to and usage of company knowledge (63 percent) and to steal intellectual property (32 percent). Malicious users may gain access to confidential information, resulting in data breaches. Unauthorized users have carried out malware attacks on the victim's IP address or physical server, according to Farad Sabah[14]. The nefarious plan could range from theft to retaliation. In a cloud environment, an insider may disrupt whole networks, as well as exploit or steal data. Systems that depend solely on a protection cloud service provider are the ones who are most vulnerable.

- Backup and Storage

The cloud vendor should make sure that data is backed up on a regular basis and that all security measures are in place. However, backup data is frequently found in an unencrypted state, posing a risk of unauthorised access to the information. As a result, data backups are associated with a number of security risks. The more server virtualization is used, the more difficult it becomes to backup and store data [15]. One method for reducing backup and offline storage volumes is to use data de-duplication.

- Service hijacking

Unauthorized users having unlawful control of such approved services is known as service hijacking. Phishing, malware manipulation, and theft are just some of the methods that can be used. This is only one of the dangers. Account hijacking [16] has been described as one of the most serious attacks. Since the account is not in its original tongue, the chances of it being hacked are incredibly high.

- VM Hopping

The attacker can monitor the VM's resource procedure of the victim/user, alter the configurations and can even delete sensitive storage data, thus endangering the confidentiality, integrity, and accessibility of the VM. The intruder must be able to recognise the IP address of the target VM and both VMs must be running on the same host for this form of attack to work. Though PaaS and IaaS users have little control, an intruder may use benchmark client capacities to pick a user's IP address by employing a variety of tricks and combinatorial inputs. As a result, VM hopping in cloud storage may be considered a rational hazard.

A. The deployment model's security issues

- Protection problems with platform-as-a-service (PaaS)

PaaS allows the deployment of cloud-based systems without the requirement to buy and manage the underlying hardware and software layers [17]. PaaS cannot function without a stable and reliable network. The two software layers that make up PaaS protection functionality are also the security of the PaaS network itself as well as the security of consumer applications installed on a PaaS platform.

- Third-party relationships

In addition to standard scripting languages, PaaS incorporates third-party web services elements such as mashups [18]. Repositories are a category of framework that integrates several source elements into a single entity. As a consequence, PaaS architectures have protection problems relevant to mashups [19]. Mashups are a kind of mashup that combines many source elements into a single integrated entity. As a result, PaaS models pose security vulnerabilities connected to mashups. [20] The protection of web-based programming platforms as well as third-party service providers is crucial for PaaS users.

- Development Life Cycle

From the perspective of application creation, developers can encounter the challenges of creating stable applications that can be hosted in the cloud. The rate at which cloud systems evolve would have an effect on both the protection period and the SDLC [21]. Software developers must bear in mind that PaaS apps must be improved on a regular basis, so they must maintain that their programme creation systems are scalable enough to keep up with improvements. However, software developers should be aware that any modifications to PaaS modules can jeopardise the security of the programme. Developers must be trained and knowledgeable on data legal questions, in addition to safe software practises, to ensure the data is not processed in insecure locations. Records can be stored in a variety of locations, each with its own set of legal requirements for privacy and protection.

- Security of facilities

At PaaS, software developers usually do not have access to the underlying layers, so vendors are in control of both the hardware and the application facilities. Developers, on the other hand, have no assurance that the resources offered by a PaaS vendor for production environments are safe, even though they have access controls.

- Resource Pooling and Cloning

Clone is a term that refers to the act of replicating or duplicating records. Cloning will result in data leakage, revealing the machine's validity. Pooling of resources is defined by Wayne A. Pauley[22] as a service that allows users to access a variety of resources and distribute them based on their application need. Instead of network replication, resource pooling entails unauthorized entry. Virtual and cloud computing research shows that even a virtual computer can be conveniently provided, reversed, interrupted, restarted, and migrated between two machines, posing unauditable security risks.

- Data unencrypted

Data protection is a process capable of solving various foreign and disruptive challenges. Unencrypted data is particularly susceptible to confidential data since there is no encryption framework. Unauthorized users can access unencrypted data rather quickly. This data loss risks personal data for unauthorised users to escape various data details from a cloud server[23]. For example, the Drop Box was alleged to use a single encryption key for all user data held by the firm. These unsafe, unencrypted files promote the manipulation of data in one manner or another by malicious users.

- Authentication and management of identity

Using the cloud, a user can access private data and make it accessible throughout the network to various services. Management of identity helps users to authenticate their credentials. The major issue of IDM is its interoperability drawback as just a result of multiple authenticity tokens and procedures for negotiating identity as well as the architectural model [24].

- Network Issues

Cloud computing makes use of the Internet and remote servers to store data with a variety of applications. Any piece of information that needs to be submitted goes via this network. Security problems with the cloud network have been illustrated by H.B. Tabakki[25]. Digital resources, fast connectivity, and on-demand applications are all available to customers. This cloud's network structure is vulnerable to various attacks and security problems, including cloud malware injection attacks, web browsing security concerns, flood attacks, locks-in, unreliable data removal, data privacy and wrapping in XML signature elements.

- 1XML Signature Element Wrapping

It is a famous web service attack. This provides protection the identification and host name against unlawful parties but does not protect the position in documents[26]. The intruder uses SOAP messages and shredded data that the user does not understand to threaten the host machine. The XML wrapping attack modifies the content of the signed message, but not the text itself. The customer will be unable to comprehend as a result of this.

- Browser Security

The browser is used by the client to submit network data. SSL technology is used by these browsers for user authentication and certificates. Hackers on the intermediate server, on the other hand, can obtain these credentials by sniffing packets on the intermediary host. You may have a single identity, but this certification should enable users to use digital authorizations to achieve various degrees of assurance.

- Flooding Attacks

In this type of assault, the invader sends a large number of requests for services to the Server in a short period of time, causing the cloud to become overburdened. According to an IBM[27] report, the cloud has the ability to scale up and down on request. It grows in response to invader demands to render services inaccessible to ordinary users.

- SQL Injection Attack

These attacks are considered to be malicious on cloud computers, with malicious code being injected into SQL code. This intrusion allows a hacker to obtain unauthorised access to a computer and other classified information. SQL injection may be used to target any kind of SQL database. Since SQL injection and other vulnerabilities are possible, this is due to a lack of focus on security during development.

V. LIMITATIONS AND CHALLENGES ON SECURITY CLOUD TESTING

As in preliminary phase of the new approach of cloud computing, most researchers focused on broader and more coherent understanding, which included definitions, challenges, and benefits[28]. The safety of cloud environments was subsequently one of the main concerns in adopting and using new technologies. The recent RightScale Inc. [29] revealed that the second highest security concerns in cloud computing are security challenges. Distributed systems may be targets for attacks that cause radical additional charges, such as data changes and downtimes. Data loss or leakage accounts for 24.6% and 3.4% of threats from cloud-related malware to [30]. Most incidents with software security are vulnerabilities exploited[31] therefore recommends the development of security measures to identify vulnerabilities.

Implemented systems should therefore be tested using analysis techniques and engineering principles to detect safety problems as soon as possible . However, one of the biggest challenges in cloud-testing environments is safety tests according to Nachiyappan & Justus[32] also indicated that there are many open queries in the current cloud security testing, such as quality assurance and security validation. The authors also indicated the challenge of testing safety actions in cloud environments. Kumar & Singh[33] has revealed the problem of quality inspections in cloud environments. In addition, the developer need to develop a cloud privacy testing approach. The literature review reveals an enormous gap in sophisticated safety testing approaches for cloud testing, although the body of knowledge on cloud testing grows. Researchers focused mainly on testing the cloud as a service (TaaS).

VI. REAL LIFE EXAMPLES

- Target

During the year 2013, a Target security attack exposed the credit card details of nearly 70 million customers. Target's network compromise, including iCloud's, exposed a number of protection flaws in the company's policy. The Target hack was the product of an HVAC contractor tracking store climate systems gaining access to the network, but after the Target device had been compromised, the hackers merely uploaded a grabber software to mirror payment data to an inaccessible Target server. For two months, hackers had connections to the payment stream, which was brimming with personal details from holiday shoppers. Target was hit with a $400 million deficit, as well as a significant loss in consumer confidence. The CEO's work was jeopardised as a result of it. In 2013, hackers had obtained access to Target's network for almost two weeks. While Target has taken steps to close any security gaps, the breach should have been prevented. This assault had been predicted by an intrusion detection system on many occasions, but the alerts were ignored.

- Home Depot

The loss caused by Home Depot's assault was much worse, with more than 56 million credit or debit cards and nearly 53 million emails stolen. Over a six-month stretch, ransomware gained access to a POS device, allowing hackers to gain access to Home Depot's networks. Hackers gained entry to Home Depot's network by using the username and password of a third-party provider. Hackers then gained greater rights that permitted them to navigate sections of Home Depot's system and instal custom-built malware on the company's self-checkout systems in the United States and Canada, using the stolen credentials to gain direct access to the organization's point-of-sale computers. Including the fact that these files did not include any passwords or other personal material, phishing scams remain a serious danger.

- Sony

Hackers known as the Guardians of Peace gained access to details ranging from employee information to emails and unreleased films. Furthermore, the assault resulted in the destruction of several of Sony's machines and servers. Malware was discovered to be the source of the chaos on Sony's network. Though malware defence is critical and may have definitely minimised the damage, in-depth network security intelligence is essential for gaining a deeper understanding of what is going on a network. In the case of an attack, network surveillance will warn enterprises, but these warnings are useless if attacks are ignored. The Sony hack was not caused by the cloud; rather, it was caused by insufficient network protection measures.

- Other Cases

In 2011, Google had a major outage, which resulted in the loss of approximately 150,000 Gmail users' addresses, contacts, and other material. It was affected, according to Google, by a tech update that had unintended effects. It took Google four days to fully recover the data of the impacted customers, which is a long time considering that the incident reportedly affected fewer than 1% of Google accounts. Customers of the Microsoft Business Productivity Online Suite storage service were allegedly able to retrieve details on other suite customers unwittingly after a data leak was revealed in 2010. The software giant believed that the problem had been fixed within a few hours of its detection and that only a few consumers had been affected.

Acknowledgment

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the System and Network Security Research task. This study was supported by the Ministry of Higher Education Malaysia and the Universiti Utara Malaysia.

References

[1] L. Riungu-Kalliosaari, O. Taipale, K. Smolander, and I. Richardson, “Adoption and use of cloud- based testing in practice,” *Softw. Qual. J.*, vol. 24, no. 2, pp. 337–364, 2016.

[2] M.M. Mosbah, “Current Services In Cloud Computing: A Survey,” *Current Services in Cloud Computing: A Survey,” International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, vol. 3, No.5, no. October2013, Nov. 2013.

[3] M. et al Armbrust, *Above the clouds: A Berkeley view of Cloud Computing”*. UC Berkeley EECS, 2009.

[4] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, “Scientific cloud computing: Early definition and experience,” in *2008 10th IEEE International Conference on High Performance Computing and Communications*, 2008, p. 825830.

[5] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”,” in *In Proceedings of IEEE International Conference on Services Computing*, 2009, pp. 517–520.

[6] A. Choudary, “Cloud Computing Services: A Deeper Dive Into Cloud Computing,” *edureka*.

[7] T. G. (nist) Peter Mell (NIST), “The NIST Definition of Cloud Computing,” Sep. 2011.

[8] D. Jamil and H. Zaki, “Security Issues in Cloud Computing and Countermeasures,” *International*.

[9] T. G. (nist) Peter Mell (NIST), “The NIST Definition of Cloud Computing,” no. October 25, 2011, Sep. 2011.

[10] J. W. Rittinghouse and J. F. Ransome, “Security in the Cloud,” CRC Press, 2009.

[11] T. Garfinkel and M. Rosenblum, “When virtual is harder than real: Security challenges in virtual machine based computing environments,” vol. 10, pp. 227–229.

[12] F. Sabahi, “Cloud Computing Security Threats and Responses”,” IEEE, 2011, pp. 245 – 249.

[13] S. Oza, “Denial-of-Service (DoS) Attacks — Web-based Application Security, Part 7,” *Spanning*, 15-Jun-2020. [Online]. Available: https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/.

[14] M. A. Morsy, J. Grundy, and I. Müller, “An analysis of the Cloud Computing Security problem,” 2010.

[15] Intel IT Center, “Preparing your Virtualized Data Center for the Cloud,” 2017.

[16] C. Keene, “The Keene View on Cloud Computing,” *Blogger.com*, 14-Dec-2009.

[17] J. F. R. John W. Rittinghouse, *Cloud Computing*. CRC Press.

[18] Wesley Chai, Kate Brush, & Stephen J. Bigelow, “PaaS (platform as a service),” *techtarget*, May-2021. [Online]. Available: https://searchcloudcomputing.techtarget.com/ definition/Platform-as-a-Service-PaaS.

[19] W. A. Pauley, *Cloud Provider Transparency – An empirical evaluation”, the IEEE computer and reliability societies*. IEEE, 2010.

[20] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”,” *IEEE transactions on parallel and distributed systems, IEEE, Digital Object Indentifier*, vol. 10, p. 1109, 2011.

[21] R. C. R. D. Bhattacharjee, “A Survey on Cloud Computing Security, Challenges and Threats,” *International Journal on Computer Science and Engineering*, vol. 3, pp. 1227 – 1231, Mar. 2011.

[22] Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez and Andrés Marín, “Enhancing Privacy and Dynamic Federationn IdM for Consumer Cloud Computing,” *IEEE Transactions on Consumer Electronics*, vol. 58, No. 1, pp. 95 – 103, Feb. 2012

[23] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[24] T. M. S. K. Latif, *Cloud Security and Privacy*. O’Reilly Media, Inc., 2009.

[25] “Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments,” 2010, pp. 393– 398.

[26] D. Jamil and H. Zaki, “Security issues in cloud computing and counter measures”,” *International Journal of Engineering Science and Technology (IJEST*, vol. 3, no. 4, pp. 2672–2676.

[27] “IBM United Kingdom,” *Ibm.com*. [Online]. . [Accessed: 13-Jun-2021]. http://www.trl.ibm.com/projects/web20sec/

[28] Armbrust, “Adoption and use of cloud-based testing in practice,” 2010.

C. P. Mature, “State of the cloud report,” *Digitalrealty.com*.

https://www.digitalrealty.com/resources/rightscale-2016-state-of-the-cloud-report

[29] E. T. Matthew K. O. Lee, “A Trust Model for Consumer Internet Shopping,” *International Journal of Electronic Commerce*, pp. 75–91, 2013.

[30] B. Akhgar, “EUROPEAN INTELLIGENCE AND SECURITY INFORMATICS CONFERENCE 2016,” August 17 – 19th 2016.

[31] J. S. Nachiyappan Subramanian, “Cloud Testing Tools and its Challenges: A Comparative Study,” *Procedia Computer Science*, Dec. 2015

[32] S. K. &. Singh, “Role of Cloud ERP on the Performance of an Organization: Contingent Resource Based View Perspective,” pp. 659–675, May 2018.