BFH1925020F

by Iftekhar Efat

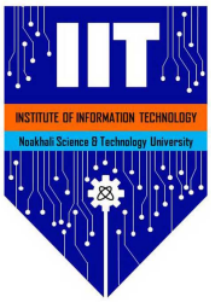
Submission date: 13-Mar-2022 01:58AM (UTC-0500)
Submission ID: 1782992550
File name: BFH1925020F.pdf (354.44K)
Word count: 1924
Character count: 10613

Vulnerabilities of cloud computing systems in 2022

Aupa Das Shormi
BFH1925020F

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University



Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

Cloud computing has recently gotten a lot of interest because of its adaptability and inexpensive maintenance costs. Cloud computing currently encompasses all components, including end-users, networks, access management, and infrastructures. We look at the most popular cloud computing platforms, as well as the vulnerabilities that have been discovered, and evaluate the effect of these flaws. Then the impact of the vulnerabilities discovered so far for each cloud computing paradigm may be shown.This analysis depicts the period during which cloud computing solutions piqued the interest of users and those looking to hack them.These solutions still have some flaws, and effort is currently being done to improve cloud computing security.

1 Introduction

Cloud computing is a network of parallel and distributed computing systems made up of a collection of interconnected and virtualized computers that are made available to businesses and individuals on a dynamic basis. The first Cloud Computing premises debuted in the 1950s, when powerful computers were enormous and required a lot of physical space to be installed. Cloud computing is a well-developed computer technology area that enables cost-effective and scalable computing service growth. Due to the expensive expense of acquiring a computer, many businesses have hired time to use one — a practice known as "time-sharing." Cloud computing provides on-demand computing, database storage, software applications, and other IT services over the Internet nowadays. By 2023, the total amount of money in the cloud market is expected to reach 623.3 billion dollars.

Although there are numerous advantages to using Cloud Computing, there are also some substantial obstacles to overcome. Security is one of the most major impediments to adoption, followed by concerns about compliance, privacy, and legal difficulties . Because Cloud Computing is such a novel computing model, there is a lot of confusion regarding how security can be achieved at all levels (e.g., network, host, application, and data) and how applications security can be migrated to Cloud Computing . Because of this uncertainty, information executives have frequently stated that security is their top concern with Cloud Computing .

Cloud computing brings with it a slew of new security concerns and obstacles. Data is kept with a third-party source and accessed via the internet via the cloud. This means that data visibility and control are restricted. It also begs the question of how it can be safeguarded correctly. Everyone must be aware of their responsibilities as well as the security risks associated with cloud computing.

---

2 COMMON CLOUD COMPUTING VULNERABILITIES AND EXPOSURES

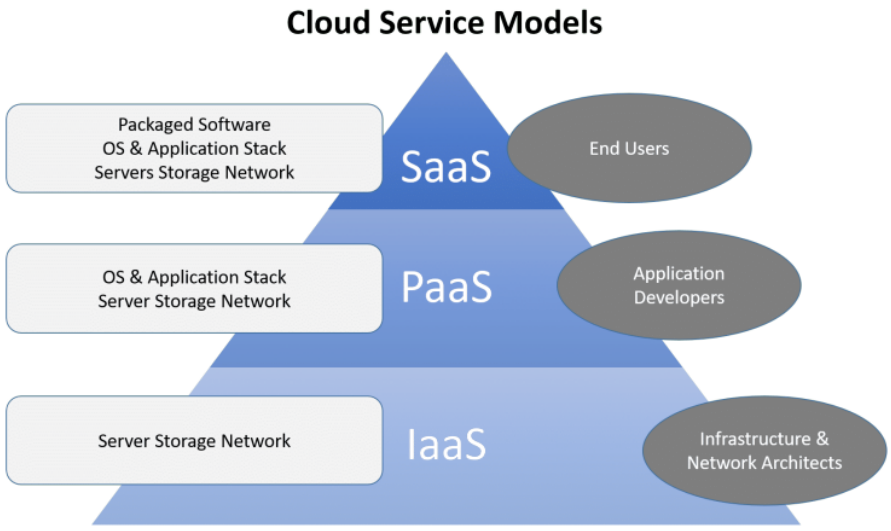
CVE stands for Common Vulnerabilities and Exposures, and it is a standard for publicly disclosed vulnerabilities and exposures. All of the main IT vulnerabilities discovered so far are stored in the CVE vulnerability base. A new vulnerability is described and given a unique identifier in the CVE list shortly after it is identified.

SaaS: Software as a Service: In the cloud industry, Software as a Service, often known as cloud application services, is the most widely used choice for organizations. SaaS makes use of the internet to distribute programs to users that are controlled by a third-party vendor. The majority of SaaS services run immediately in your web browser, thus there are no client-side downloads or installations required.

Employees and businesses benefit from SaaS because it reduces the amount of time and money spent on time-consuming operations like installing, managing, and upgrading software. This frees up a significant amount of time for technical staff to focus on more critical topics and issues within the company.

There have some downside also like interoperability,vendor lock-in,data security,customization,lack of control,feature limitations,performance and downtime.

PaaS – Platform as a Service: Platform as a Service (PaaS) is a cloud computing category that allows industry vendors to create and build applications and services over the Internet by providing a platform and environment. Platform as a service (PaaS) services are hosted in the cloud and can be accessed by users via a browser. PaaS allows users to construct software applications using tools provided by the vendor. Customers can subscribe to preconfigured features in PaaS services, or they can opt to include only the features they need, those that satisfy their needs, and leave out the rest.As a result, PaaS packages can range from basic point-and-click bidding, which requires no hosting skills, to providing the whole infrastructure with complex development possibilities.



IaaS – Infrastructure as a Service : Infrastructure as a Service (IaaS) is a type of cloud gives access to computer resources in a "Cloud" virtualized environment via a public connection, commonly via the Internet; the computing resources given are particularly virtualized hardware resources, in other words the

infrastructure, as with any cloud computing services. Virtual server space, network connections, bandwidth, IP addresses, and load balancing are examples of IaaS services.The hardware resource pool is accessed via a variety of servers and networks that are usually deployed over numerous data centers, and its maintenance is handled by the IaaS service provider. In order to develop their own IT systems, the client is given access to virtualized components.

3 Security Issues

Application Security :
Typically, these programs are supplied via the Internet using a Web browser . Web application weaknesses, on the other hand, may expose SaaS applications to vulnerabilities. Attackers have been exploiting the internet to get access to users' computers and carry out destructive operations such as data theft . SaaS applications face the same security concerns as any other online application technology, but typical security solutions are ineffective in protecting them from assaults, necessitating new techniques . The 10 most serious online application security threats have been recognized by the Open Web Application Security Project (OWASP) . There are more security concerns, but it's an excellent place to start when it comes to securing web apps.

Data Security : Data security is a typical problem for any technology, but it becomes a significant challenge when SaaS users have access to sensitive information. should put their trust in their service providers for adequate security . Organizational data is frequently processed in plaintext and saved in the cloud while using SaaS. The SaaS provider is the company that provides the software as a service. One who is in charge of data security while is processing and archiving . In addition, data backup is a must.Important factor to consider in order to make recovery easier in the event of a disaster.It's a calamity, but it also raises security issues .Other services, such as security, can also be subcontracted by cloud providers.As a backup from third-party service providers, who may or may not be able to bring up concerns.

Platform-as-a-service (PaaS) security issues : PaaS allows cloud-based applications to be deployed without the expense of purchasing and maintaining the underlying hardware and software layers . PaaS, like SaaS and IaaS, requires a secure and dependable network as well as a secure web browser. PaaS application security is divided into two layers: PaaS platform security (i.e., runtime engine) and PaaS platform security (i.e., client apps installed on a PaaS platform) . The platform software stack, which includes the runtime engine that runs the customer apps, is the responsibility of PaaS providers. PaaS, like SaaS, has its own set of challenges, including data security.

Accessibility : Using a web browser to access apps over the internet simplifies

access from any network device, including public computers and mobile devices. However, it also increases the security concerns associated with the service. The Cloud Security Alliance has published a document that describes the current state of mobile computing and the top threats in this area, including data-stealing mobile malware, insecure networks (WiFi), vulnerabilities found in device OS and official applications, insecure marketplaces, and proximity-based hacking.

Infrastructure-as-a-service (IaaS) security issues:

IaaS provides a virtualized system that has a pool of resources such as servers, storage, networks, and other computing resources that can be accessed via the Internet. Users have complete control and administration over the resources allotted to them, allowing them to run whatever software they want. As long as there are no security holes in the virtual machine monitor, cloud users have more control over security with IaaS than with previous models.They are in charge of the software that runs on their virtual machines and of correctly configuring security settings. Cloud providers, on the other hand, are in charge of the underlying compute, network, and storage infrastructure. To limit the vulnerabilities posed by creation, communication, monitoring, modification, and mobility, IaaS providers must make a significant effort to safeguard their systems. Here are a few of the security concerns with IaaS.

4 Conclusion

As cloud computing becomes more widespread, upgrades and other technical advancements may be implemented more quickly and efficiently. It has the potential to provide innovators with a wider choice of scalable tools for research, development, and testing than they would otherwise have access to. Because new technologies are always vulnerable, it's critical to assess the existing solutions' weaknesses and dangers.

We examined the existing common vulnerabilities for the key cloud computing solutions in this article, which covered all three cloud computing models: IaaS, PaaS, and SaaS.

We feel that such an alliance is critical for the advancement of technology, as this advancement must be tied to particular security norms. Existing vulnerabilities for the solutions in use must be presented and assessed so that there is no risk of these vulnerabilities being present in the solutions in question. The amount of vulnerabilities found indicates that people are interested in these solutions. Those attempting to identify new vulnerabilities will be interested in a solution if it is used. There are solutions available that do not have a huge number of flaws. This does not imply that the answer is completely risk-free, but it may indicate that it is uninteresting.

[2] [3] [1]

References

[1] Said El Kafhali, Iman El Mir, and Mohamed Hanini. Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering*, 29(1):223–246, 2022.

[2] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, and Eduardo B Fernandez. An analysis of security issues for cloud computing. *Journal of internet services and applications*, 4(1):1–13, 2013.

[3] Alin Zamfiroiu, Ionut Petre, and Radu Boncea. Cloud computing vulnerabilities analysis. In *Proceedings of the 2019 4th International Conference on Cloud Computing and Internet of Things*, pages 48–53, 2019.

BFH1925020F

ORIGINALITY REPORT

49%	35%	4%	44%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jisajournal.springeropen.com Internet Source	7%
2	www.coursehero.com Internet Source	5%
3	v1.overleaf.com Internet Source	4%
4	Submitted to University of Sunderland Student Paper	4%
5	Submitted to Federal University of Technology Student Paper	4%
6	Submitted to North West University Student Paper	3%
7	Submitted to Bahrain Training Institute Student Paper	3%
8	Submitted to Kent Institute of Business and Technology Student Paper	2%
9	Submitted to Sheffield Hallam University Student Paper	2%

10	Submitted to King's Own Institute Student Paper	1 %
11	Submitted to Southern New Hampshire University - Continuing Education Student Paper	1 %
12	Submitted to Kaplan College Student Paper	1 %
13	global.oup.com Internet Source	1 %
14	Submitted to University Tun Hussein Onn Malaysia Student Paper	1 %
15	Submitted to Da Vinci Institute Student Paper	1 %
16	Submitted to Roehampton University Student Paper	1 %
17	www.ijstr.org Internet Source	1 %
18	annalsofrscb.ro Internet Source	1 %
19	link.springer.com Internet Source	1 %
20	Submitted to Central Queensland University Student Paper	1 %

21	Submitted to Colorado Technical University Online Student Paper	1 %
22	Submitted to Harrisburg University of Science and Technology Student Paper	1 %
23	docshare.tips Internet Source	<1 %
24	www.business.com Internet Source	<1 %
25	Chandu Thota, Gunasekaran Manogaran, Daphne Lopez, Vijayakumar V.. "chapter 12 Big Data Security Framework for Distributed Cloud Data Centers", IGI Global, 2017 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

BFH1925020F

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 3

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Prep. You may be using the wrong preposition.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 4

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

PAGE 5

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Missing "," You may need to place a comma after this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to remove this article.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Sentence Cap. Remember to capitalize the first word of each sentence.

Article Error You may need to use an article before this word.

PAGE 6

Article Error You may need to use an article before this word.

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

PAGE 7