Security Issues and Challenges in Cloud Computing Services

Lakshmi Venkata Raghava Sudheer Devanaboina
Department of Telecommunications
Blekinge Institute of Technology
Karlskrona, Sweden
lvr0899@gmail.com

Yashwanth Venkata Sai Kumar Adabala
Department of Telecommunications
Blekinge Institute of Technology
Karlskrona, Sweden
yashwanthadabala26@gmail.com

***Abstract*— This paper deals with the security issues and challenges that are impacting distinctive characteristics of cloud computing. Cloud computing is one of the most important on Internet of Services and computer infrastructure. Cloud computing provides resources and shared services through the internet. Services are delivered through the data center. Finally, this paper analyzes the security threats, challenges related to data security, privacy of the user, and virtualization stack in cloud computing.**

Keywords—security issues, cloud computing services, security issues in cloud computing

I. Introduction

Cloud computing is a modern technology which is currently rapidly being adopted throughout the world in many businesses, organizations. In the last few years cloud computing has grown from being a promising business concept to one of the fastest growing segments of IT industry [1]. Cloud Service Providers (CSP), i.e., Microsoft, Google, Amazon are leveraging virtualization technologies combined with self service capabilities for computing resources through the internet [1]. The National Institute of Standards and Technology in America (NIST) has defined cloud computing as a service model for universal access with a minimum interaction with the service provider [2]. Cloud is basically providing IT resources which are on demand through the internet. There are different forms of cloud such as private cloud and public cloud. Since Cloud computing comprises distributed networks, the computing environment in a cloud scenario is prone to the same risk as any other computer network. Cloud computing can also be defined as an assembly of distributed and a parallel computer system containing an interconnected resource [2]. The cloud computing provides the resources as per the needs of the consumer. We know that for any organization or an industry, the information is its major property. People save their information in secure place or in different types of storage devices. The storage devices are of many types. The most recent type of storage device is the cloud. Cloud computing is understood as a virtual cloud with an infinite amount of storage to provide service. The cloud can be divided based on the type of computing or based on the type of services it offers.

The cloud computing provides rich benefits to the cloud clients such as costless services, elasticity of resources, easy access through internet, etc [3]. Even though cloud computing has enormous benefits the users of cloud are not willing to put their personal details or any confidential information such as personal health records, emails and government sensitive files.

II. Research Method

A Systematic Literature Review (SLR) as a research study method is used to evaluate and interpret the research topic's available literature.

A. Research Questions

1) *RQ1: What are the cloud computing security threats?*
2) *RQ2: What are the security issues that are related to the virtualization stack?*
3) *RQ3: What are the security problems that have not been addressed by commercial cloud providers?*

B. Data Sources

The data sources used for this SLR are as follows:

1) *IEEE Xplore*
https://bibliotek.bth.se/databases/go/ieee
2) *Scopus*
https://bibliotek.bth.se/databases/go/scopus
3) *Springer*
https://bibliotek.bth.se/databases/go/springer
4) *Science direct*
https://www-sciencedirect-com.miman.bib.bth.se/

C. Search Strategy

The databases IEEE Xplore, Scopus, Science direct and Springer were chosen to select studies for this review because they have provided an easier search mechanism through their respective search engines, which we utilized by entering certain keywords related to the SLR. The search strings used are:

"Security issues in cloud computing"

"Cloud computing"

"Challenges in cloud computing"

"Security issues and challenges in cloud computing"

We have selected the papers using snowballing method.

D. Inclusion and Exclusion Criteria

Inclusion Criteria:

1. Research studies that include cloud computing.

2. Research studies that discuss cloud security issues.

3. Research studies that include cloud security models.

4. Studies that are written in English.

Exclusion Criteria:

1. Studies that are published in other than the English language.
2. Papers with unidentified references.
3. Articles focusing on other than security topics of cloud computing.
4. Duplicated research paper.
5. Studies that are not clearly related to any defined research question.

5. *Work Division:*

All the work that must be done for this SLR is done together by both of us throughout the process of completing this SLR.

Related work:

1. Security threats in Cloud Computing:

Data loss due to its leakage is a severe threat to cloud security. When the cloud computing begins to run out, data is stored in a location other than the client computer and this data turns from one run to multiple runs. With these changes there is a risk of leakage or loss of information [4]. Data compromise and modifications occur without keeping the backup copy by altering or deleting the original information. Also, data storage on cloud media has less reliability because insiders and third parties can access the data. In irresponsible media, the companies' offering of cloud service are regarded as fraudulent. Utility based approach can be used to overcome the latter-mentioned challenge by detecting the malicious behaviour of users. This utility allows users to recover their data. Unity service is a personal repository service, which is different from other cloud services. Cloud services users do not need to become unauthorized users of services, but internal individuals of Cloud Service Providers (CSP) organization present malicious behaviour. In studies [5] we have found such incidents, which can harm the data security from cloud service providers. Therefore, trust-building between client and cloud service providers is emphasized through a unity model. The concept of software and services is activated on the users' demands. However, several additional risks have been perceived by the productive organization. A hacker can perform tricks to snatch the confidential information as each and every thing is kept inside the cloud computing box. Due to evolution in the security disciplines, hackers can be prevented to have an illegal access to cloud data. Also, more security measures can be proposed to provide a comprehensive security to users regarding their data. The key-splitting and Homomorphic encryption can be extended to have new breakthroughs in this area of research [5]. In [6], the emphasis was on secure data transfer between customers and cloud computing providers over the secured communication channels.

Data storage, data confidentiality, and data availability in cloud services are among the other identified threats to cloud computing security. For example, outsourcing stored data at the cloud requires an additional security layer to strengthen the data confidentiality. Research [7] introduced a ''cloud storage based on ID-based encryption'' (CS-IBE) with the one file access policy and a user's identity proposed to be used as an encryption key. Although this approach simplifies the key management issues, it shows limited performance for data confidentiality.

A recently published work [1] introduces a new cloud service, namely ''database as a service'' (DBaaS), where a service provider has responsibility to grant access of software, hardware, and network to users. It would enable them to access and manage a database. At the same time, a distrustful service provider keeps the control of database queries. As a result, security issues emerge in the confidentiality of stored data during outsourcing of data to a user. The important threat that a cloud storage security faces is the inside attack. The person inside the same company causes a problem to the security of the data [8].

Security Challenges/ Security issues	Data Storage	Identity Management and Access Control	Contractual and Legal Issues
1.	Data privacy and Integrity	Malicious Insider	Service Level Agreements
2.	Data Recovery and Vulnerability	Outside Intruder	Legal Issues
3.	Improper Media Sanitization		
4.	Data Backup		

Research Question 1 Summary table:

Research Question	Papers which include RQ1
Security Threats	[1],[2],[4],[5],[6],[7],[8],[9]

2. Security issues related to virtualization stack:

Most of security threats identified in a virtual machine environment are very similar to the security threats associated with any physical system. The following are some general threats that are unique to the virtual environment [9].

A. *Attack between VMs or between Virtual Mchine (VMs) and Virtual Machine Monitor (VMM)*

One of the primary benefits that virtualization brings is isolation. This benefit, if not carefully deployed will become a threat to the environment. Poor isolation or inappropriate access control policy will cause the inter-attack between VMs or between VMs and VMM.

B. *VM escape*

Virtual machine escape (VM escape) is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker accessing to the host operating system and all other VMs running on that host.

Virtual machines are allowed to share the resources of the host machine but still can provide isolation between VMs and between the VMs and the host. New software bugs were already found to compromise isolation. One such example of this kind of attack is VM escape.VM escape is one of the worst case that happens if the isolation between the host and between the VMs is compromised. In the case of VM escape, the program running in a virtual machine is able to completely bypass the VMM layer and get access to the host machine. Since the host machine is the root of security of a virtual system, the program which gain access to the host machine also gains the root privileges basically escapes from the virtual machine privileges.

C. *Virtual machine controlled by Host Machine*

Host machine in the virtual environment is considered to be the control point and there are implications that enable the host to monitor and communicate with the VM applications up running. Therefore, it is more necessary to strictly protect the host machines than protecting distinctive VMs. Different virtualization technologies have different implications for the host machine to influence the VMs up running in the system.

D. *Denial of Service*

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used with regards to computer networks but is not limited to this field; for example, it is also used in reference to CPU resource management.

Research question 2 summary table:

Research Question	Papers which include RQ2
Security issues related to virtualization	[5],[9],[10],[13],[15]

3. Security problems that have not been addressed by commercial cloud providers:

A survey study [10] finds that the top five cloud providers, including Amazon, Azure, Adobe, Google cloud platform, and VMWare, are efficient in their cloud services' data security feature. Reliability and performance are among other features. To measure the cloud providers' trustworthiness is still an issue for researchers, and a customer cannot judge it without appropriate tools. Container launched by Virtual Machines (VMs) is an emerging practice offering security sandboxing. Containers enable the cloud providers to continue managing their applications on clouds [11]. Since application management at the edge is challenging for cloud providers, it is done either ad hoc or with the platform. When multi-tenant run their applications on the same host resource, security, and privacy issues arise from their applications. Existing literature on cloud service providers (CSPs) reveals that cloud service models are involved in hampering security concerns [12]. Therefore, it is users' workload based on the sensitive data that they do not need to outsource to a public cloud directly. Outsourcing the consumers' data and addressing the associated risks is challenging for both users and cloud service providers. These risks include shadow-IT, security, control and transparency, and business continuity [13]. Interoperability is another challenge because many consumers are locked to a single CSP due to interoperability issues. Amazon AWS ''Identity and Access Management'' (IAM) [9] operate the access control mechanism and identity management system. Each customer gets a tenant account upon the subscription of the Amazon AWS product. To assure the security of users' data, they are allocated security credentials to access AWS resources. However, Amazon IAM is not so expressive and contains simple featured-based policies with the limited encryption attributes. AWS and Microsoft Azure policies clearly state that customers need to address the security of their data, operating system, application, and their configuration, identity, and access management in a shared responsibility. The AWS only considers the hardware, software, and networking facilities security [5]. Cloud users mistakenly assume that their public IaaS providers have responsibility for securing their data, operating system, and applications [14]. ''Secure by design'' [8] is an innovative idea that needs to be integrated with all cloud services and applications to enable an agile environment for businesses in the face of security threats and the technology ecosystem. Thus, researchers can undertake future research to develop security architecture to ensure built-in security from developing systems and services, tools, and technologies across the cloud environment. Before the latter mentioned studies, a research article [15] focused on software security requirements and proposed replacement of traditional software development with the emerging services. Thus, cloud providers can share a security service with the distributed stakeholders.

Research question 3 summary table:

Research Question	Papers which include RQ3
Security problems that have not been addressed by commercial cloud providers.	[5],[6],[9],[10],[11],[12],[13],[14],[15]

Conclusion:

The cloud problems are mainly with the security and privacy of the data stored in the cloud. The cloud environments like heterogeneity, resource sharing, multitenancy, virtualization, mobile cloud computing and Service Level Agreement (SLA) that makes the cloud security more vulnerable. This paper provides the different security threats that are there. There are also new developments in cloud computing like Container-as-a-Service (CaaS), Software-defined networking (a concept to design and manage networks that abstracts applications away from the underlying networks), Software-defined-storage (abstracts the logical storage services and capabilities away from the underlying hardware) and Cloud-of-Things (CoT), (a concept combining cloud computing and Internet-of-Things (IoT) for smart city applications). All these new developments bring new challenges in cloud computing, and they need to be addressed. When there is a change in technology, always review the security policies and procedures and update accordingly to protect the data and its privacy.

References

[1] D. P. Singh, P. Kaushik, M. Jain, V. Tiwari, and S. Rajpoot, “Data Storage Security Issues in Cloud Computing,” in 2021 International Conference on Innovative Practices in Technology and Management (ICIPTM), Greater Noida, India, Feb. 2021, pp. 216–220. doi: 10.1109/ICIPTM52218.2021.9388321.

[2] T. Moyo and J. Bhogal, “Investigating Security Issues in Cloud Computing,” in 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems, UK, Jul. 2014, pp. 141–146. doi: 10.1109/CISIS.2014.21.

[3] N. vurukonda and B. T. Rao, “A Study on Data Storage Security Issues in Cloud Computing,” Procedia Computer Science, vol. 92, pp. 128–135, Vijayawada, India, Jan. 2016, doi: 10.1016/j.procs.2016.07.335.

[4] S. M. Shariati, Abouzarjomehri, and M. H. Ahmadzadegan, “Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection,” in 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran, Nov. 2015, pp. 1078–1082. doi: 10.1109/KBEI.2015.7436196.

[5] K. Popović and Ž. Hocenski, “Cloud computing security issues and challenges,” in The 33rd International Convention MIPRO, Opatija, Croatia, May 2010, pp. 344–349.

[6] N. Kshetri, “Privacy and security issues in cloud computing: The role of institutions and institutional evolution,” Telecommunications Policy, vol. 37, no. 4, pp. 372–386, Greensboro, USA, May 2013, doi: 10.1016/j.telpol.2012.04.011.

[7] A. Bentajer, M. Hedabou, K. Abouelmehdi, and S. Elfezazi, “CS-IBE: A Data Confidentiality System in Public Cloud Storage System,” Procedia Computer Science, vol. 141, pp. 559–564, El Jadida, Morocco, Jan. 2018, doi: 10.1016/j.procs.2018.10.126.

[8] A. A. Nayak, N. K. Sridhar, G. R. Poornima, and Shivashankar, “Security issues in cloud computing and its counter measure,” in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), India, May 2017, pp. 35–41. doi: 10.1109/RTEICT.2017.8256554.

[9] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing,” Procedia Computer Science, vol. 125, pp. 691–697, Kurukshetra, India, Jan. 2018, doi: 10.1016/j.procs.2017.12.089.

[10] H. Alhadawi and M. Zolkipli, “Data security issues in cloud computing: review,” International Journal of Software Engineering & Computer Systems (IJSECS, vol. 2, pp. 2289–8522, Pahang, Malaysia, Mar. 2016, doi: 10.15282/ijsecs.2.2016.5.0016.

[11] M. Alshehri, “An Effective Mechanism for Selection of a Cloud Service Provider Using Cosine Maximization Method,” Arab J Sci Eng, vol. 44, no. 11, pp. 9291–9300, Dhahran, Saudi Arabia, Nov. 2019, doi: 10.1007/s13369-019-03947-y.

[12] H. Tianfield, “Security issues in cloud computing,” in 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, Korea, Oct. 2012, pp. 1082–1089. doi: 10.1109/ICSMC.2012.6377874.

[13] R. Bhadauria and S. Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques,” IJCA, vol. 47, no. 18, pp. 47–66, India, Jun. 2012, doi: 10.5120/7292-0578.

[14] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On Technical Security Issues in Cloud Computing,” in 2009 IEEE International Conference on Cloud Computing, Germany, Sep. 2009, pp. 109–116. doi: 10.1109/CLOUD.2009.60.

[15] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Syros, Greece, Mar. 2012, doi: 10.1016/j.future.2010.12.006.