*International Journal of Engineering & Technology, 7 (2.32) (2018) 131-135*

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# A Survey on User Awareness of Cloud Security

**Dr. Gudapati Syam Prasad (Professor)[1], Vidya S. Gaikwad (Research Scholar)[2]**

*[1,2]CSE Department, K L E F, Vaddeswaram, Guntur, Andhra Pradesh, India – 522502*
**Corresponding author E-mail: syamprasad.gudapati@gmail.com*

**Abstract**

The cloud computing technology provides cost effective, powerful computation resources on the fly. It minimizes the need to procure and maintain expensive hardware, software and reserve space for IT infrastructure. These features for cloud computing encourages organizations and individuals to migrate their resources needs and services to the cloud. However, cloud computing services provided by third-party vendors possesses various security threats. The cloud services store sensitive data (such as credentials, personal information, etc.) of various users on the shared environment that escalates security concerns. The aim of this research survey paper are three-fold: i) provides guideline for researchers who are new to the cloud computing security area, ii) provides the state-of-the-art survey of cloud computing security issues and challenges, and iii) provides the further research directions required into security assurance of the cloud computing.

***Keywords***: *cloud; security; characteristics; attacks; counter measures; , challenges in cloud security, cloud computing, security*

## 1. Introduction

A cloud computing and storage of data on cloud is ubiquitous in past few years, where users are preferring to store their personal data such as photographs, bookmarks, music files, personal documents, etc on cloud servers. Virtualization technology is a backbone of cloud computing, but was limited only on mainframe servers[1, 8]. Virtualization allows effective and efficient management of resources such as hard disks, processor, network devices, memory, etc available in the servers of a data center. Cloud computing integrates virtualization concept for management of servers and resources, whereas software layers provide seamless and transparent interface to users to perform various activities such as computation, storage, etc. Using virtualization and software layers, cloud computing provides the essential charchartierstics such as scalability, location independence, elasticity, resource pooling, and pay-as-you-use.

The software layer manages network traffic and resources demands and based on the demand it dynamically creates new servers or destroy unnecessary ones in data centers to meet the demands of users or applications. Therefore, security layer implementation is also an essential component of a management layer. To protect users data and confidential information from various kinds of attacks.

It is important to understand the cloud security challenges in a systematic way to address cloud security issues:
1. It is necessary to inspect and investigate various cloud vulnerabilities, threats and risks.
2. It is necessary to clearly identify security requirements such as CIA triad, authentication, authorization, etc.
3. Identify all the stakeholders and role of each stake holder in the attack-defense process; and
4. Understand how various cloud deployment models (public, community, private, hybrid) are affected by the security threats and challenges.

According to the Symantec threat report 2017[14], there is 91% increase in attacks that targeted for certain victims. Some research efforts try to remedy the problems. For example, certain network-based attacks are now detected and prevented[15, 16].

### Contributions

In summary, this research survey work makes the following contributions:

- Summarizes the state-of-the art research in the cloud computing security.
- Provides analysis of various attacks and countermeasures in the cloud computing.
- Provides research directions and guidelines for implementing various security solutions on the cloud computing platform.

The rest of this research paper is organized as follows: Section 2 describes characteristics of the Cloud Computing. Section 3 discusses the general requirements of cloud computing security. Section 4 provides user survey on Cloud Computing Security. Section 5 provides comparative analysis of attacks and countermeasures. Section 6 lists various research questions and challenges in the Cloud computing, and we conclude the paper in Section 7.

## 2. Characteristics of Cloud

There are three types of service modes available in the cloud computing as shown in Figure 1:

**Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.**

- **Infrastructure as a Service (IaaS)**: It allows users to dynamically request for computing, data storage, networking and other computing resources. In addition, it also provides freedom to users to run operating system of their choice using virtualization technology. The users of IaaS have capability and can monitor and control the usage of their deployed applications, storage, computation requirements, networking capabilities, etc.

- **Platform as a Service (PaaS):** It allows the users and provides flexibility to users to deploy the applications tools that are supported by the provider. As compared to IaaS, in PaaS users do not have freedom to manage the underlying cloud infrastructure such as networks, servers in data centers, operating systems (OS), storage, etc. Whereas, in PaaS deployed applications and hosting environment provided to the application are controlled by the user.

- **Software as a Service (SaaS):** This mode of cloud computing is mostly used by the users and it provides users with a capability to user provider's application hosted on cloud servers. The applications are accessible for various platforms such as mobile devices, desktop devices, servers and mainframes using a web browser. In this mode, users do not have flexibility or capability to control the underlying cloud infrastructure including operating system, storage, network devices, or application capabilities. Users can not modify the hosting environment where applications are hosted. Users are limited and restricted to modify or manage only application specific setting to customize their own profile.

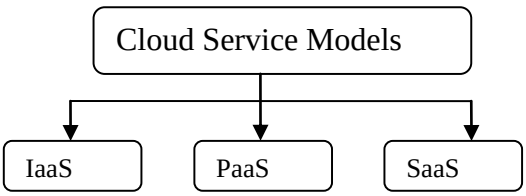


**Fig1**: Types of Cloud Service Models

The cloud computing offers four different deployment models for cloud architecture solutions as shown in Figure 2 and described below:

- **Private cloud**: This type of cloud infrastructure provided, operated and managed by a private organization. The management of the cloud infrastructure can be done by organization itself or a third party. The cloud infrastructure may be hosted on premise or off premise.

- **Community cloud**: The Community cloud infrastructure is shared among the several users. It supports a specific community that has communal concerns (e.g., security requirements, missions). The community cloud can be managed by an organization or a third-party. It can exists on premises or off-premises. It is a multi-tenant platform that allows several users or organizations to work on the same platform proved that they have similar concerns and requirements. Examples of community cloud are Microsoft Government Community Cloud and Google Apps for Government.
- **Public cloud**: The public cloud is managed and owned by an organization that is providing or selling the cloud services to general users. It is available to general public Examples of public cloud include but not limited to Amazon Elastic Compute Cloud (ES2), Sun Cloud, IBM's Blue Cloud, Google's App Engine and Windows Azure. A simple example of public cloud could be an electronic email.

- **Hybrid cloud**. This type of cloud infrastructure uses mix of cloud computing platforms such as private cloud and community or public cloud, whereas these different cloud platforms are blinded using standards and technologies to make applications portable and compatible on these mix cloud platforms. A business application designed for hybrid cloud by an organization connect mix environment of public cloud, private cloud or community cloud as they were a single environment and provides transparent service to users by hiding the underlying details. The cloud is not called as a hybrid cloud if a few programmers of an organization using public cloud for testing the prototype of an application which is completely disconnected from the private cloud or data center. A hybrid cloud means an organization exchanges data between a private cloud or application environments.

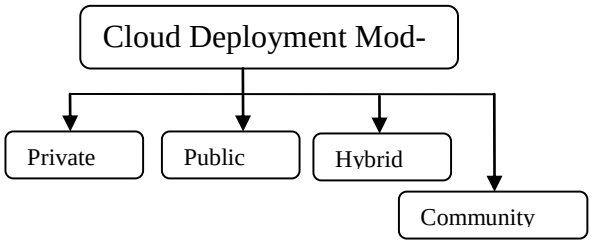


**Fig** 2: Types of Cloud Deployment Models

A number of key characteristics of cloud computing have been identified [3,4]:

- **Flexibility/Elasticity**: Cloud computing allows its users to dynamically request for computing resources such as processors, storage, memory as needed without requiring any human intervention. Automatically, resources are rapidly and elastically allocated and assigned to users based on the requirements of users to scale up or down.
- **Scalability of infrastructure**: Based on the requirements of application or organizations new servers or computing resources in form of new nodes can be easily added or removed from the network as can physical servers, without human intervention and disruption in exiting services. According to the demand requirements, the cloud architecture allows scaling horizontally or vertically.
- **Broad network access**. Cloud computing resources and services are available to an organization or users to access over the network using heterogeneous platforms(e.g., mobile phones, laptops).
- **Location independence**. Cloud computing seamlessly stores data at different location around the world. Users usually do not get a freedom to choose the exact location of the provided resources. (e.g., country, state, or datacenter).
- **Reliability**: Using replication of data on multiple servers located at same or different site provides reliability to users and this unique feature makes cloud computing popular among users and disaster recovery.
- **Cost Effectiveness**: To lower the cost, usually cloud deployments are often located near cheap power station. Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale.
- **Sustainability**: It is provided through comes about through improved resource utilization and more efficient systems.

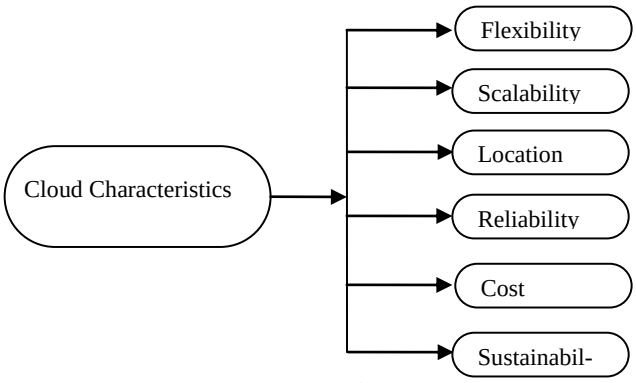


**Fig** 3: Characterization of Cloud Computing

Figure 3 illustrate the characterization of Cloud computing.

## 3. General Requirements on Cloud Security

Three important characteristics of security are confidentiality, integrity and availability. The other characteristics of security includes trust, audit and compliance.

1. **Confidentiality**. Confidentiality refers to only authorized users or application will be able to access protected data. Confidentiality characteristics ensures that unauthorized users or applications will not be able to access the data stored on the cloud. In cloud computing data is stored on remote servers that are owned by service provider and shared by multiple users. However, cloud computing ensures to make secure logical compartments with security checks to ensure isolation of users data on same servers to protect confidentiality of users data. The users data can be stored on the single server or multiple servers at same or different sites. The threat to confidentiality increases in the cloud due to large number of users haring the same resources on the cloud, therefore, it is necessary to create secure compartments for isolation of data and ensuring and auditing their security strengths timely manner is important in cloud computing. It is also necessary to establish policy to perform regular security checks to validate confidentiality of users' data[12].
   To ensure confidentiality various encryption techniques are proposed by researchers and adopted in cloud computing. There are two types of algorithms: symmetric or asymmetric encryption algorithms. The key length and key management in case of the symmetric cipher are important characteristics of an encryption algorithm. This is dependent on cloud service provider and algorithms adopted by them. Also, the cloud service providers should ensure deployment of encryption methods and standards using NIST standards in [5].
2. Integrity. Integrity is critical security property of Cloud computing. Integrity means that data stored on cloud can be modified only by authorized parties or in only the authorized ways allowed by an application. Integrity is associated with users data, application and hardware. Data Integrity refers to protecting users data from unauthorized access and modification. The integrity protection methods and techniques provide information about who may have altered the data and what data is altered [11].
3. Availability. Availability ensures that system is accessible upon demand by an authorized user. In other words, availability refers to that a user has access to complete set of allocated cloud resources at all times. Availability can be affected temporarily or permanently. A loss incurred due to unavailability of resources can be partial or complete. The threats to availability includes denial of service (DOS) attacks, and equipment outages. The natural disasters is also a threat to availability [13].
   The cloud computing needs various sensors as well as machine learning based techniques to ensure availability of researches to users is achieved. Availability concerns also extend to the need to migrate to another provider, uptime periods of current provider or long-term viability of the cloud provider [6] [7].
4. Trust. Trust is important factor in cloud computing. It is depends on self-assessment and perception of reputation of cloud service providers. Various techniques, model and tools have be proposed to establish trust. However, there are very few research efforts to analyze trust relation among cloud services providers cloud users.
5. Audit and Compliance: Auditing is the mechanism to review and examine all records and attempts of cloud resources authorization and authentication to check for compliances with security standards and policies. A cloud service provider should have policies to ensure and inspect customer needs and security of data and cloud cloud infrastructures is intact. A cloud service provider should perform external audits and security certification and penetration testing [1,2].

## 4. User Survey

To identify user requirement security features in cloud computing and awareness of users on the attacks and countermeasures of cloud computing we conducted a user survey of 300 engineering students to understand the user perception and preferences regarding cloud computing. The survey included following five questions. Each user is offered with the same set of questions and answer choices.

Would you prefer to host your sensitive data on cloud platform? Fig 4 indicates the result of survey. Total 50 users preferred to host sensitive data on cloud computing, 56 users prefer not to host sensitive data on the cloud platform and 5 user simply don't care.

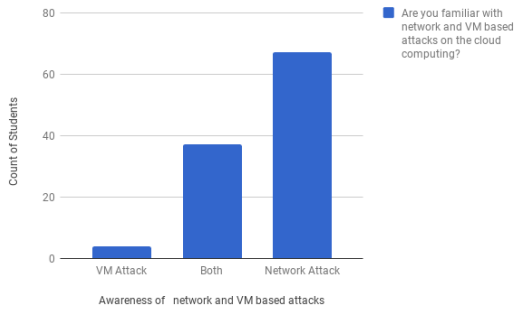


**Fig**. 4 Survey result sensitive data hosting on cloud.

Are you familiar with network and VM based attacks on the cloud computing? Fig. 5 indicates the result of the survey. According to the survey result, only 67 users were familiar with n/w attacks, 4 users knew VM attacks and 37 users were familiar with both network and VM attacks.

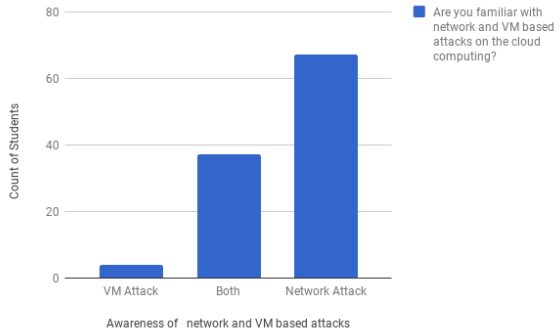


**Fig**. 5 Survey result of users awareness about N/w and VM attacks on the Cloud platform

Are you familiar with countermeasure applied by various cloud service providers to protect against attack? Fig. 6 presents the result of the survey. Majority of the users are unfamiliar with the countermeasure used by the cloud service providers, whereas they have intrinsic assumption that cloud service providers might have state-of-the-art countermeasure in place and their data will be secure.

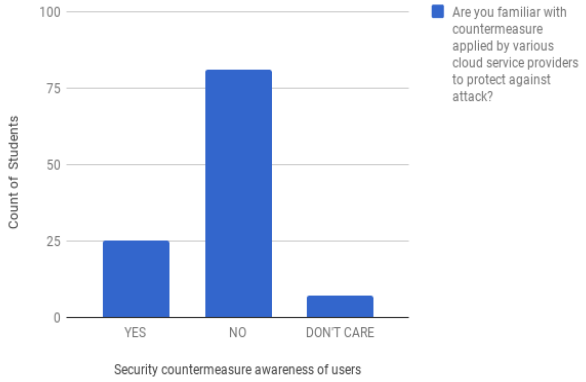


**Fig**. 6. Survey result of security countermeasure awareness of users

Have you seen service level agreement of cloud service providers? Fig. 7 shows the result of the survey. It reveals that many users tend to ignore reading of service level agreement hence don't know in details what service guaranties are offered by the cloud service providers.

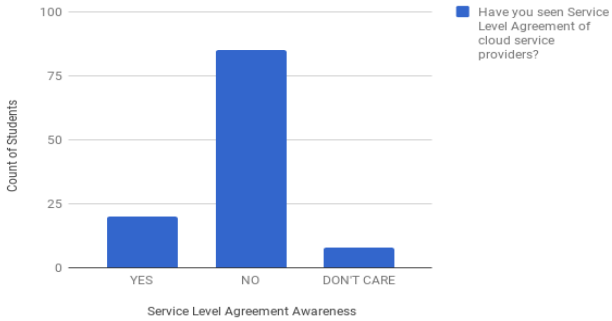


**Fig**. 7. Survey result of service level agreement awareness of users

Do you feel attacks and security incidents should be reported by cloud service provider to its users? Fig. 8 shows result of the survey where majority of the users prefer not to be annoyed by incident reporting and it should be taken care by cloud service providers.

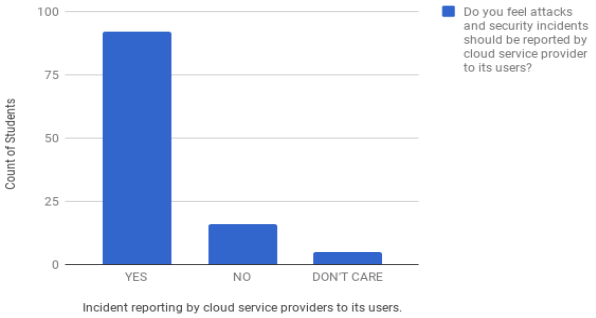


**Fig**. 8. Survey result of incident reporting by cloud service providers to its users.

This user survey reveals that the implicit trust by users on cloud service providers and negligence to read to service level agreement puts sensitive data on the risk, Hence, it is critical to study various attacks and countermeasure for cloud computing platform. What are your main concerns in your approach to the Cloud Computing?

- Privacy
- Availability of services
- Integrity of data
- Confidentiality of data
- Unclear scheme in the pay per use apporach
- Cost and difficulty of migration to the cloud

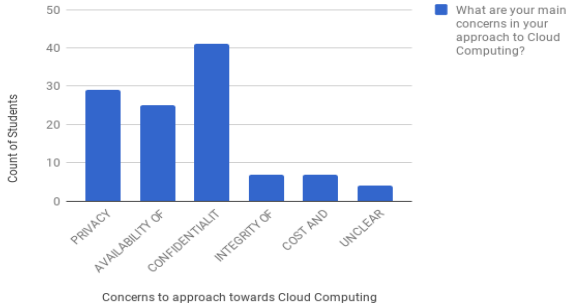


**Fig**. 8. Survey result of major concerns in approaching to cloud computing

## 5. Comparative Analysis of Attacks and Counter Measures

Using various service deployment models cloud services are provided to users by cloud service providers. The attacks on cloud computing are possible on various layers of service model. Therefore, it is necessary to apply counter measure at various layers to ensure security at various levels of cloud deployment model. The attacks on cloud computing violates security properties and possess threat to users data on cloud storage.

This section lists and analyzes various research works that reveal attacks on clouds and their counter measures.

Network based attacks and counter measures: Various attack techniques are used by botnets to successfully exploit the cloud infrastructure to get unauthorized access to data and resources. In addition, botnet use cloud services to launch attacks and store data. For instance, the well-known Zeus botnet was revealed to be using Amazon's Elastic Computing Cloud (EC2) as command and control server (McMillan, 2009). The Zeus botnet targeted to steal users credentials. Its ZITMO variant has been found to be used for illegal bank transactions. Similarly, the Google cloud platform App Engine has been used as a botnet to communicate with the infected computers (Info Security, 2009).

In [9] presented a method for detecting botnets in cloud. It used an approach to determine the cryptographic keys being used for communication between bots and Command & Control servers. It is achieved by spreading Pebbleware, an executable malware code that identifies the host machines. Botnet server tracing mechanism successfully worked on the well-known Zeus botnet.

VM based attacks and counter measures: By modifying the executable code, security of a virtual machine being copied to create another VM may be compromised (Garfinkel and Rosenblum, 2005). An attacker can inject worms/viruses in the original VM before creating a copy of the VM (Morsy et al., 2010). It is a difficult task to trace origin of the vulnerability of attack in a newly created VM.

Various research efforts [3,4,6] proposed a technique to detectvarious VM based attacks and the misuse patterns.

Storage based attacks and counter measures: Cloud uses replication to keep data. In [10], the authors have described the various attacks related to data reduplication in the cloud that are providing storage services. Whenever a resource allocated for a

user is reallocated to another user, it causes the data scavenging [5]. Even though, new allocation is performed still both the data and storage of the previous user may become accessible to the new user. Thus, the data scavenging is responsible for the violation of data protection.

## 6. Research Questions and Challenges

This section provides a brief overview of research challenges in the cloud computing.

1. Scalability: The scalable solutions provides an ability to increase the storage of data or number of users or number of connection of the system in a systematic manner. Distributed data storage is a preferred mechanism in cloud platform for enterprise solutions, it makes NoSQL a popular choice for distributed data storage on the cloud platform.
2. Ensuring Availability: As cloud environment is shared among multiple users and number of users are increasing due to popularity of cloud computing and services offered at cheap cost, this implies cloud service providers ensure delivery of data wherever it is requested by authorized users. This requires research efforts to investigate what models could to deployed on the cloud to ensure delivery of big-data and big-data analysis on the cloud, while ensuring high density of availability.
3. Data Integrity: Data integrity is a key aspect of security in the cloud computing. Major challenges are how to ensure correctness of user's data in the cloud at any time interval. How cloud data is assessed on a regular interval to ensure security and integrity of data stored on the cloud.
4. Privacy: Privacy of user data and personal sensitive information stored on the cloud platform has become a serious concern due to deployment of big data mining and analytics techniques. An investigation and standard framework is required to ensure privacy of users data on the cloud platform.
5. How IOT or Wearable systems[17] data is securely communicated to the cloud using middlewares.

## 7. Conclusion

Cloud computing provides various services to its users using effective and efficient utilization and sharing of underlying resources. However, security threats and issues of cloud computing are the major bottleneck and hindering its prevalence. This research work presented a survey of cloud computing security issues, threats and challenges. This paper discusses the modes of cloud computing, characteristics of cloud and the security for the cloud. This paper also discusses about the vulnerability to cloud and their counter measures. This research papers serves as a guidelines for potential researchers that are exploring in the cloud security domain.

## References


[1] E. Naone, "Technology overview, conjuring clouds", MIT Technology Review,July–August, 2009.

[2] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.

[3] G. Reese, "Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: Theory in Practice", O'Reilly Media, 2009.

[4] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing" as the 5th utility, Future Generation Computer Systems (2009).

[5] L. M. Kaufman, "Data security in the world of cloud computing", IEEE Security & Privacy, vol. 7, no. 4, 2009, pp. 61-64.

[6] R. Chow, "Controlling data in the cloud: Outsourcing computation without outsourcing control". In ACM Workshop on Cloud Computing Security, 2009.

[7] J. Brodkin, "Gartner: Seven cloud-computing security risks". In: Infoworld 2008 http://www.infoworld.com/d/securitycentral/gartnersevencloudcomputing- security-risks-53?page=0, 1

[8] Vishal Meshram, Vidula Meshram and Kailas Patil, "A Survey on Ubiquitous Computing", ICTACT Journal on Soft Computing, Vol. 6, No. 2, pp. 1130-1135, 2016.

[9] Chow, R.; Golle, P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R.; Molina, J. Controlling data in the cloud: Outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security, Chicago, IL, USA, 13 November 2009; ACM Press: New York, NY, USA, 2009; pp. 85–90.

[10] Samarati, P.; di Vimercati, S.D.C. Data protection in outsourcing scenarios: Issues and directions. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), Chicago, IL, USA, 4–8 October 2010; ACM: New York, NY, USA, 2010; pp. 1–14.

[11] Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. J. Internet Serv. Appl. 2013, 4, 5.

[12] ] S. Lins, P. Grochol, S. Schneider, et al.,"Dynamic certification of cloud servic‑ es: trust, but verify,"IEEE Security & Privacy Magazine, vol. 14, no. 2, pp. 66- 71, 2016. doi: 10.1109/MSP.2016, 2016.

[13] J. Tang,"Ensuring security and privacy preservation for cloud data servic‑ es,"ACM Computing Surveys (CSUR), vol. 49, no. 1, article 13, Jul. 2016.

[14] Symantec. (2017). Internet security threat report [Online]. Available: https://www. symantec.com/security_response/publications/monthlythreatreport.js

[15] W. Lin and D. Lee ,"Traceback attacks in cloud—pebbletrace botnet,"in IEEE International Conference on Distributed Computing Systems Workshops, 2014, pp. 417-426

[16] A. Web, S. Overview, and S. P. May. (2009, Jun.). Amazon web services: over‑ view of security processes [Online]. Available: https://fenix.tecnico.ulisboa.pt/ downloadFile/3779573805259/AWS_Security_Whitepaper.pdf

[17] K. Patil, Q. Jawadwala and F. C. Shu, "Design and Construction of Electronic Aid for Visually Impaired People," in IEEE Transactions on Human-Machine Systems, vol. 48, no. 2, pp. 172-182, April 2018. doi: 10.1109/THMS.2018.2799588