Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2023)
IEEE Xplore Part Number: CFP23CV1-ART; ISBN: 978-1-6654-7451-1

A Review on Cloud Security and Its Challenges

Sai Balaji Mallisetty[1]
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Greenfields, Vaddeswaram, Guntur, 522302, India
saibalajimalisetty@gmail.com

Gnana Amrutha Tripuramallu[1]
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Greenfields, Vaddeswaram, Guntur, 522302, India
gnanaamrutha1701@gmail.com

Kanksha Kamada[1]
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Greenfields, Vaddeswaram, Guntur, 522302, India
kankshakamada2002@gmail.com

Pooja Devineni[1]
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Greenfields, Vaddeswaram, Guntur, 522302, India
devinenipooja1102@gmail.com

Dr. S. Kavitha[1]
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Greenfields, Vaddeswaram, Guntur, 522302, India
kavithabtech05@gmail.com

Dr Anne Venkata Praveen Krishna[2]
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Greenfields, Vaddeswaram, Guntur, 522302, India
praveenkrishna@kluniversity.in

2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) | 978-1-6654-7451-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/IDCIoT56793.2023.10053520

***Abstract*—Cloud security has recently become more prevalent in industry. Cloud security combines security and cloud computing. Many firms use cloud computing to store enormous volumes of data and to manage their business systems. There are four different classifications of cloud security, including governance, compliance, availability, data security and identity and access management (IAM) etc. To illustrate how each industrial job might be interconnected, cloud security architecture and their objectives such as Advanced Encryption Techniques, Unified Visibility for private, hybrid and public cloud, Enhanced Identity and Access Management, Virtual Firewall are discussed. Security is required when storing the records but there are many complications and limitations to provide security, major challenges in providing cloud security are cyberattacks, misuse of cloud resources, lack of cloud security plans, unsecure API, to solve these challenges in cloud a variety of security techniques are used. Next, both users and operator's security implications of cloud security are looked at. In order to meet the problems faced by cloud security, numerous technical solutions such as virtual firewall, authentication controls, protection policies are used.**

Keywords— Cloud Computing, Cloud Security, Privacy Protection, Security Threats

I. INTRODUCTION

One of the biggest changes in technology in our generations is cloud computing. The introduction of cloud technology has fundamentally changed how businesses are conducted in the modern world. Everyone is looking forward to the new economy's future investment."cloud computing" can be defined collective pool of computing resources that require minimum maintenance effort or communication with cloud providers, and may be easily installed and deployed.The name "cloud" actually comes from telephone since in the 1990s, a telecoms provider that had previously primarily provided point-to- point data lines started providing VPN services(VPN also known as Virtual Private Network) with a similar level of service but at a considerably cheaper price.

The scientific and business communities are becoming more aware of the expanding significance of cloud computing. According to a Gartner survey [1], cloud computing was ranked as the first among the top 10 technologies and had a better probability of being adopted by companies and organizations throughout time.

Network connectivity to a variety of programmable computer sources(apps and services) is made possible by cloud computing that may be quickly provided and deployed with no administration help.

With all resources represented as services and distributed over the Internet, Cloud computing is represented as a computational framework in addition to a distribution structure, and its main goal is to provide security , rapid and simple data storage and cloud computing services [2,3]. The cloud improves cooperation, agility, scalability, availability. It also helps speed up development work and offers the possibility of cost savings through targeted and profitable computing [4–7].

Adopting cloud computing has many advantages, but there are also some major obstacles to overcome . Some of the challenges are security, followed by problems with privacy and legal issues [8]. There is a lot of misunderstanding on how security may be achieved at all levels and how applications security is transferred to cloud computing because cloud computing is a new type of computing(technology)[9]. Information executives frequently cite security as their top issue with relation to cloud computing due to this uncertainty [10].

In a variety of architectures, under various service models, the use of cloud technologies can cohabit together other techniques and methods for software creation. Additional aspects of cloud computing, such as resource distribution, data management, and multi-tenancy have not only exposed new security issues but also sustain to the system's existing defences[11]. In addition to provide governments, businesses, and individuals with secure cloud computing services, it is essential to conduct an acceptable security evaluation study on the impact of cloud computing.

The Literature survey that has been performed by various team members has been mentioned in the Section II.

The definition and different Cloud Architecture are proposed in Section III, along with an overview of the cloud security market. Section IV examines a variety of cloud users and their roles , limitations regarding security in the cloud infrastructure and other security issues. Section V will follow by the security solutions and conclusion at the end.

II. LITERATURE REVIEW

Several websites have been reviewed so that we can understand the foundations of cloud technology and maintaining the security of data in the respective cloud. The review of the literature in this section establishes a starting point for talking about various elements of cloud security.

Amrutha and Pooja provided pretty good insight into cloud computing's core concepts. This article explores the fundamentals of cloud technology and it also can also assist the growing world in utilizing the cutting-edge innovation [1].
Balaji and Pooja, on the other hand, have talked about the security issues that users of the cloud face [2].
Amrutha and Balaji claim that security concerns are one of the main barriers keeping big businesses from moving their data to the cloud. The authors' analysis of concerns relating to cloud data security and privacy protection is excellent [3]. They have also talked about some of the options for resolving these problems [4-6].

Table 1: Comparison of Survey Papers throughout the years

Year	Covered Technology	Current Research Works
2017	IOT	Access Control
2018	Cloud (In medical)	Encryption
2019	Cloud Computing	Encryption, Access Control
2019	Blockchain	Trust, Reputation
2020	Web Security and Data Dumping	Encryption, Access Control
2021	Cyber Security in cloud	Encryption, Protection
2021	Web Security	Protection
2022	Cyber Security	Protecting from unauthorized access
2022	Cloud (In Security)	Encryption, Access Control, Trust

III. CLOUD ARCHITECTURE

Both modest and huge businesses utilize cloud technology to hold data and make it available at any time and from any place with network connectivity. The architecture of cloud computing combines event-driven and service-oriented architecture.

Cloud architecture is divided into two segments:
The client makes use of the front end. It includes client-side interfaces and software necessary for accessing cloud computing platforms which helps organizations to test and build the applications and also helps to recover, backup, analyze and store data. Tablets, smartphones and web servers make up the front end.

The provider of the service makes use of the data access layer (also commonly known as the backend). Large -scale data storage, security measures, virtual machines, deploying models, servers etc. are all included.

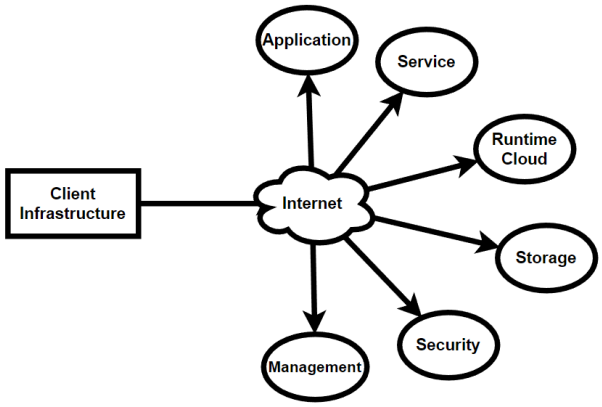

Figure 1: Architecture of Cloud Computing

A. Service Models in Cloud

- Infrastructure as a Service (IAAS)

IAAS is a type of cloud computing that makes use of the internet to deliver virtualized computer resources. On behalf of its clients, a 3rd supplier hosts hardware, software, storage and other components of the infrastructure in an IAAS architecture. IAAS providers also groups are designed like system maintenance, backup, and resiliency planning, as well as hosting users' applications. IAAS platforms are particularly suited for workloads that are transitory, experimental, or subject to unforeseen change since they provide incredibly flexible resources that can modified on-demand. IAAS setups also feature dynamic scaling, desktop virtualization, automated administrative duties, and policy-based services. To manage unforeseen resource needs, the infrastructure can scale up or down dependent on application usage. Dynamic Scaling is key advantage among all cloud service model types. According to the user requirement IaaS helps in scale up or scale down of resources based on consumption. The resources and costs are minimized as a consequence of this adaptability. IaaS also helps user by providing basic building blocks to build needed applications and their infrastructures which helps the user in scaling their application/infrastructure according to their required needs. automation of administrative activities, dynamic scalability, virtualization software, and policy-based services are other features of IAAS.

Technically, there isn't much of a barrier to entry for the IaaS industry, but setting up and maintaining the cloud infrastructure could cost a lot of money. People can access open-sourced cloud infrastructure frameworks which offer a solid software foundation for businesses looking to create their own private clouds or enter the public cloud market.

- Platform as a Service (PAAS)

Software (Applications) are delivered via internet using the cloud computing architecture known as Platform as a Service (PAAS). In PAAS model, a provider offers hardware and software tools to their users by charging them, often those required for application development. On its own infrastructure, the hardware and software are hosted by a PAAS provider.

Instead of replacing a company's whole infrastructure, PAAS relies on service providers for critical functions like hosting applications. Customers only need to log in and use the framework which is typically accessed through a browser because a Cloud vendor takes care of all the underlying software and calculation. PAAS providers charge for that access by using pay-per-use model by removing the requirement for users to install proprietary hardware and software, PAAS frees users from having to create or execute new application but consumption of resources by the user might be determined in various ways based on a fixed price per user and a finite set of custom integration objects, one provider may charge.

- Software as a Service (SAAS)

Users have access to applications that are provided by a company or firm provider through a network, typically the Internet, under this paradigm for the distribution of software. As supporting techniques that allow services (Web) and SOA (Service oriented Architecture) mature and new construction approaches gain popularity, SAAS has grown to become an increasingly common delivery paradigm. IDC defines the hosted adaptive approach and the software development model as two somewhat distinct SAAS delivery strategies.

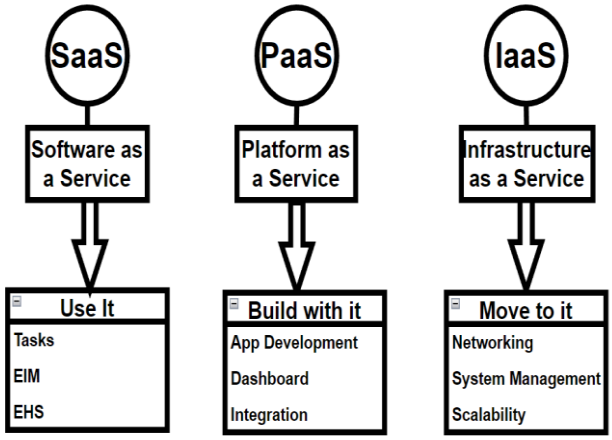

Figure 2: Service Models

B. *Deployment Models in Cloud*

- Public Cloud

The general public can utilize the public cloud to access computing resources including software and devices over the internet. For companies and organizations with little security concerns, it is a good option. As cloud computing companies configure and maintain these services, the management of these resources is not necessary. Public clouds are typically used for testing and application development.

- Private Cloud

You can utilize the resources and infrastructure for a single firm using a private cloud. Users do not exchange resources with other users or organizations. It sometimes goes by the names Internal or Corporate Model for this reason. Due to their expensive maintenance, private clouds are more expensive than public clouds.

- Community Cloud

The community deployment model and the private cloud share certain similarities. In a private cloud, the cloud server is held by just one customer or business. The Community Cloud server is distributed by a few businesses with similar histories. This multi-tenant architecture can assist organizations or businesses in cost-saving and efficiency-boosting measures if they all adhere to the same security regulations, performance standards, and objectives. The development, execution, and maintenance of projects can all be handled using this methodology.

- Hybrid Cloud

Public and private clouds are combined to create the hybrid cloud. Very few businesses and organizations are able to quickly transition to cloud computing all at once. As a result, cloud service providers developed a hybrid cloud that allows for a seamless transition between private and public cloud resources. They store non-sensitive data on the public cloud while they maintain sensitive data in the private cloud.

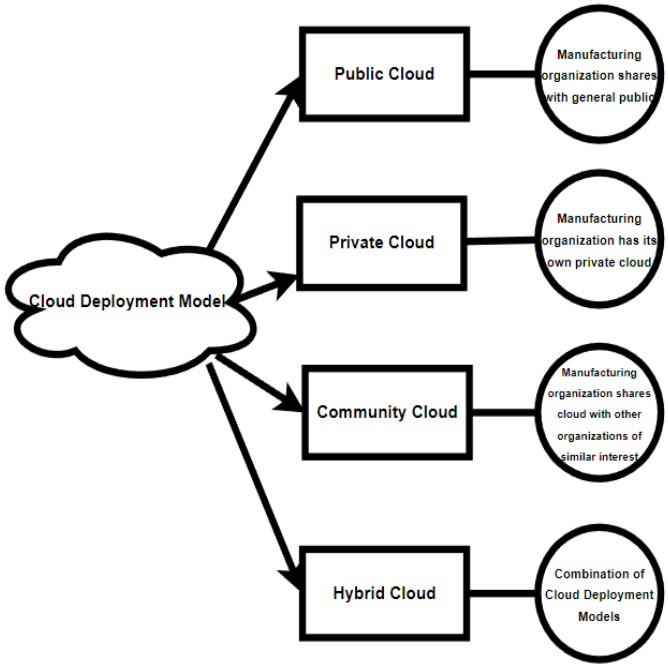

Figure 3: Deployment Models

IV. Cloud Security

This section covers topics related to cloud computing security, such as its understanding and application, job duties within the sector, and risks that cloud security poses to clients as well as operators.

A. *The definition of Cloud security*

Currently, a large number of operators are providing their individual cloud computing knowledge. In the field of cloud computing, commonly referred to as cloud security, operators will risk running across security issues. It alludes

to a massive selection of controls, technologies, and policies used to safeguard cloud computing data, applications, and supporting infrastructure. In other words, cloud issues that are associated with security risks with cloud-based computing systems, such as data encryption, privacy protection, and resource availability when security is threatened. We must ensure that all of these problems are successfully integrated and controlled if we are to guarantee the consistency of the cloud environment.

B. Cloud Computing Security Industry

It is essential to understand composition of the cloud security sector to prevent security events.

- Cloud providers

  Amazon, IBM, and Microsoft are just a few of the cloud service providers who have previously provided deployment solutions for cloud computing security in an effort to increase data protection. The majority of them rely on data encryption, auditing and ID authentication.
- Operators

  There are two ways to cloud computing security from the operator's perspective. The cloud security can be achieved through logically centralized system by fusing cloud computing and the current security mechanisms. The second method is that they might establish services to the clients that safeguard cloud computing.
- Security Vendors (Security Service Provider)

  Classic IT security companies contribute their two unique groups of cloud-based security products and solutions when they enter the cloud computing industry. While the other views the "cloud" from the perspective of customer, one does it from the point of server. Prior to reaching the client side, the goal of the former is to thwart security risks at the server level. This can also be seen as creating a massive lists system. The latter is focused on the conventional strategy. To implement terminal clients for security precautions, that is.
- Cloud Consumers

  A cloud customer is an end user who browses or accesses the services provided by Cloud Service Providers (CSP) and engages into contractual arrangements with the hosting company. Payments are made by the cloud user each time a resource is granted access. services that are measured and used by the consumer. This involves performing a security and risk evaluation for each use case of Cloud migrations and deployments by a group of enterprises with shared regulatory limitations.

  Service-Level Agreements (SLAs) are used by cloud users to outline the technical performance criteria that a cloud provider must meet. SLAs may include provisions relating to security, performance failure remedies, and service quality.

C. Security impact on the cloud consumers

Customers are ambivalent about the potential of cloud computing. They are intrigued by the flexibility that on-demand computing provisioning offers and by the capability of integrating information technology with corporate strategy. Customers are, however, also quite worried about consequences related with cloud technology if not secured properly. The above constitute dangers to the user's privacy

- Lack of Cloud Security Plans and Expertise

  For the cloud, datacentre security models are insufficient. Administrators must acquire fresh approaches and expertise tailored to cloud computing. Although the cloud may increase organisational effectiveness, it can also leave firms vulnerable if they don't have the corporate knowledge. Misunderstanding the consequences of the shared model, which outlines the security responsibilities of the cloud provider and the user, can be a sign of poor planning. This misconception could cause inadvertent security flaws to be exploited.
- Identity and Access Management

  IAM is crucial. Although it might seem clear, the devil is in the details.

  Making the appropriate roles and permissions for a company with thousands of employees is a difficult undertaking. A comprehensive IAM approach entails three steps: role design, privileged access management, and execution. Start by creating a strong role design based on the requirements of cloud users. Create the roles independently of any IAM platform. These jobs explain the work that your staff members perform, which is consistent among cloud providers. Next, a privileged access management (PAM) plan describes which roles need greater security because of their privileges. Control who has access to privileged credentials very carefully and change them frequently.
- Cyber Attacks

  A cyber-attack is an attempt to gain access to a computer network or system by cybercriminals, hackers, or other digital enemies, typically with the goal of changing, stealing, destroying, or disclosing information. Malware, phishing, DoS and DDoS, SQL Injections, and IoT-based assaults are examples of common cyberattacks that target businesses.
- Misuse of cloud resources.

  Operators might present the appearance of limitless computing, network, and storage capacity to their clients. Spammers, authors of dangerous software, and other criminals have been able to carry out their tasks with a fair amount of impunity by availing the anonymity provided by these consumption and identification models. Finding the assailant and going back in time is difficult. A malicious person might leverage the cloud's powerful processing capabilities to guess passwords

quickly and cheaply. For an operator, it is incredibly challenging to identify and stop such actions in real time.

D. Security impact on the cloud provider

- Identity and access control violations

  High levels of centralization and virtualization are possible with cloud computing. To stay up with the fast expanding availability of cloud services, operators should offer business clients greater access control and improved identity management policies.

- Encryption algorithms

  Recent years have seen an increase in cases where user private information was leaked, which has made current encryption and key management techniques vulnerable. To safeguard client data in a multi- tenant setting, they must be enhanced.

- Unsecure API

  It is common knowledge that cloud APIs serve as a link between user handsets and the cloud service architecture. Infected cloud API will likely have user private data taken and removed, and the operator won't be able to offer consumers IaaS, PaaS, SaaS services.

- Data compromise.

  Data compromise can happen in a variety of ways. A classic example is the deleting or change of files without a copy of the original material. The destruction of an encoding key is another possibility. Customers who store their data in a CSP's data center, including governments, organizations, businesses, and individuals, run the risk of having their data compromised and their service interrupted.

Figure 4: Types of Data Compromise

V. Security Solutions

Modern technical solutions for cloud security should be taken into consideration to overcome cloud security challenges.

A. Advanced Encryption Techniques

Encrypting data is one practical method of data security. Before entering the cloud, cloud encryption converts data from plain text into an unintelligible format. Encryption of data is required both in transit and at rest. Cloud service providers offer a variety of out-of-the-box encryption options for data saved in block and object storage systems. Connections to cloud storage services should be done utilizing encrypted HTTPS/TLS connections to safeguard the data-in-transit. Cloud computing platforms use platform-managed encryption keys to encrypt data by default. Customers can, however, increase their level of control by bringing their own keys and using cloud-based encryption key management services to manage them centrally.

B. Data Loss Prevention

A comprehensive security plan should include data loss prevention (DLP), which focuses on identifying and preventing data loss, leakage, or abuse due to breaches, ex-filtration, and unauthorized access. A cloud DLP is specifically made to secure businesses that use cloud repositories to store their data.

C. Unified Visibility for Private, Hybrid, and Multi-cloud environments

A cloud security solution must provide unified multi-cloud discovery and visibility, as well as ongoing intelligent monitoring of all cloud resources. This unified visibility must be capable of identifying configuration errors, security flaws, and risks to data security while offering useful information and guiding remediation.

D. Enhanced identity and access management (IAM)

Companies can provide more granular access controls and privileges by using IAM, which streamlines,automates IAM processes. IAM solutions eliminate the need for IT teams to manually deprovision accounts, monitor and adjust rights, or impose access controls. To check the customers identity and grant permission to numerous software and websites using just one set of credentials, organisations can also enable single sign-on (SSO).

E. Virtual Firewall

A virtual firewall also known as cloud firewall, which is controlled and managed entirely within a virtual space, is a firewall that offers packet scanning and analysis. On a running guest virtual environment, the VF can be used as a standard software firewall, a virtual protection apparatus developed with virtualization protection, a change with improved security abilities, or a managed program operating within the host network.

Table 2:Security Solutions

S. No	Security Solution	Description	Limitations
1	Advanced Encryption Techniques	Cloud service providers offer a variety of out-of-the-box encryption options for data saved in block and object storage systems. Connections to cloud storage services should be done utilizing encrypted HTTPS/TLS connections in order to safeguard the security of data-in-transit.	By using these Advanced Encryption Techniques network latency, traffic is increased To overcome these factors architectures, have to be designed very carefully
2	Data Loss Prevention	A comprehensive security plan should include data loss prevention (DLP), which focuses on identifying and preventing data loss, leakage, or abuse due to breaches, ex-filtration, and unauthorized access.	To prevent the data loss more snapshots and backup devices have to be created which increases the expenses
3	Unified Visibility	Unified visibility must be capable of identifying configuration errors, security flaws, and risks to data security while offering useful information and guiding remediation.	• Limited Security and Performance Monitoring • Limited Control Over Traffic to and from
4	Enhanced IAM	. IAM solutions eliminate the need for IT teams to manually deprovision accounts, monitor and adjust rights, or impose access controls.	IAM has the risk of resulting in uncomfortable access provisioning and deprovisioning, lost productivity, and even security vulnerabilities.
5	Virtual Firewall (VF)	Cloud Firewall which is also commonly known as Virtual Firewall, it is a type of security solution made especially for settings where it is difficult or impossible to install hardware firewalls, such as public and private cloud environments, software-defined networks	Cloud firewalls rely on the server reliability of the provider. Your network will be exposed to fraudulent traffic if the provider's server goes offline. Therefore, it is essential to have a backup strategy. They apply common rules. As a result, they occasionally miss software-specific problems.

CONCLUSION

Cloud computing not only creates issues but also advances security. The improvement is demonstrated in three areas: economic advancements, technological developments, and security regulation strategies. Customers, service vendors, and even government authorities should all have legitimate security needs, according to the development of technical concepts. Both cloud service providers and users have varied security requirements. All of these requirements might not be feasible. The task of figuring out how to breach the rules governing data protection is one of the most challenging ones one has to perform. In light of these required balances, we must revise our technical concepts. Growth of the sector throughout time is a reflection of the emphasis shifting from product development to services in information security. The development of services and infrastructure must replace product development for information security products. A single infrastructure and service platform can help users address a variety of security issues. The change in the market regulator's focus is reflected in the evolution of the regulations and management. Instead of traditional regulation, which is focused with safeguarding network architecture. It is crucial to remember that the alterations are improvements rather than radical departures from the existing technical paradigms.

The following best practices are recommended for operators in this case to resolve security holes in the cloud.

1. Operators need to consider safe ways to switch from a traditional platform to a cloud one without disrupting service.
2. Operators should concentrate on figuring out ways to protect data transport, isolation, storage, and recovery within their own clouds.

REFERENCES

[1] Cloud Security Alliance. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing V4.0. [Online]. Available: http://www.cloudsecurityalliance.org/

[2] J. Li, Y. Zhang, X. Chen, and Y. Xiang, ''Secure attribute-based data sharing for resource-limited users in cloud computing,'' Comput. Secur., vol. 72, pp. 1–2, Jan. 2018. K. Elissa, "Title of paper if known," unpublished.

[3] Amazon Web Services, http://aws.amazon.com.

[4] Cloud computing. http://en.wikipedia.org/wiki/Cloud_computing.

[5] Cloud computing security forum http://cloudsecurity.org/

[6] G. Al, "Cloud Computing Architecture and Forensic Investigation Challenges," Int. J. Comput. Appl., vol. 124, no. 7, pp. 20–25, 2015.

[7] Khalil, Issa & Khreishah, Abdallah & Azeem, Muhammad. (2014). Cloud Computing Security: A Survey. Computers. 3. 1-35. 10.3390/computers3010001.

[8] A. Shamir, ''Identity-based cryptosystems and signature schemes,'' in Proc. Workshop Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1984, pp. 47–53.

[9] H. Eken, ''Security threats and solutions in cloud computing,'' in Proc. World Congr. Internet Secur. (WorldCIS-), London, U.K., Dec. 2013, pp. 139–143.

[10] H. Thimbleby, S. Anderson, and P. Cairns, "A framework for modelling Trojans and computer virus infection," Comput. J., vol. 41, no. 7, pp. 444–458, Jan. 1998

[11] Z. Wei, ''A pairing-based homomorphic encryption scheme for multiuser settings,'' Int. J. Technol. Hum. Interact., vol. 12, no. 2, pp. 72–82, Apr. 2016.

[12] Cloud Security Alliance. Consensus Assessments Initiative. Accessed: Oct. 2017. [Online]. Available: https://cloudsecurityalliance.org/artifacts/ consensus-assessments-initiative-questionnaire-v3-0-1/

[13] Shah, H. and Anandane, S.S., 2013. Security Issues on Cloud Computing. arXiv preprint arXiv:1308.5996.

[14] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 3(5), 247-255.

[15] Joshi, V. (2019). Load Balancing Algorithms in Cloud Computing.