Cloud Security

Aisha A. Abba
Department of Computer Science
Middlesex University
Flic-en-flac, Mauritius
aa4786@live.mdx.ac.uk

Aisha Muhammad
Department of Computer Science
Middlesex University
Flic-en-flac, Mauritius
am3434@live.mdx.ac.uk

Kashim K. Mohammed
Department of Computer Science
Middlesex University
Flic-en-flac, Mauritius
km1396@live.mdx.ac.uk

***Abstract*—In the last decade, cloud computing has been incorporated in various industries, from Health to Military, which has been meticulously guided by exploring related technologies in the industry and academia alike. The individual and enterprise computing model have shifted from on-site infrastructure to remote data centres which is accessible via internet and managed by cloud service providers. However, this paradigm shift in computing introduces security concerns to individuals and enterprises. To increase cloud deployment, these security concerns need to be thoroughly reviewed and addressed. This paper reviews the cloud security issues and concerns , while addressing various key topics like vulnerabilities, threats and mitigations, and cloud models.**

***Index Terms*—Cloud Computing, Security**

1 Introduction

Cloud computing is a model for fast, on demand network access to a shared network. Configurable computing resource pool (e.g., networks, servers, storage, software, and services) that includes configurable computing resources. With minimum management effort or service provider involvement, it can be easily provisioned and published. Many of us are going to see a paradigm change in information technology in our lives. Current advances in the world of computation may have significantly altered the way computing, as well as definition of capital in computing. In cloud computing network, the services are generally in the premise or network of someone else and accessed Cloud users remotely (Alam, 2020).

Processing is performed remotely, meaning that a person's data and other items need to be sent to a cloud infrastructure or computer for processing, and the output is returned. Upon fulfilment of the requested processing in certain cases, it might be appropriate or at least feasible for a person to store data on remote cloud servers. This involve the following three sensitive states or situations that are of special interest in the organizational context of cloud computing:

- Transmission of confidential personal data to the cloud server,
- Transmission of data from the cloud server to the computers of the clients and
- Storage of personal data of clients on cloud servers that are remote servers not operated by clients.

Both above three cloud computing states are severely vulnerable to security breaches that make study and investigation on the security aspects of cloud computing practice an imperative. There have been a variety of different mixes that are being used in the cloud storage realm, but the basic principle remains the same – infrastructure, or services stay somewhere else with someone else's possession, and customers borrow it for the time they use it infrastructures (Chaturvedi & Gupta, 2020). On certain cases, confidential data stored on external cloud servers must also be counted. Safety has been at the forefront of secure programming activities. When it is possible for any unauthorized entity to 'snake' on any private device by means of various 'hacking' methods; the expansion of the scope to access someone's personal data via cloud storage effectively poses more security issues.

Cloud computing is unlikely to remove this expanding scope due to its existence and attitude to it. Therefore, stability has always been a challenge for cloud storage activities. Robust security and secure computing technology are not a one-off endeavour, but a continual one – which makes it important to evaluate and understand the state-of-the-art cloud computing security as a necessary activity. Cloud is primarily classified as private cloud, group cloud, hybrid cloud, and public cloud. (Mondal et. Al., 2020).

Discussion in this paper only assumes one type of cloud. There is a public cloud as this statement would match all the features of some other type of cloud. Thanks to its diverse capacity, the cloud storage solution is the fifth utility to follow the current water, gas, and telephony services, rather than simply another facility.

The research discussed in this paper is structured with a view to exploring and defining the solution to cloud storage, security problems and questions that need to be considered in this paper. Deployment to a cloud-based computing platform. The importance of security in cloud computing, security issues, cloud security threats, including architectural illustration, cloud security attacks, solutions, and critical analysis of existing solutions was considered in the context of the debate of this article.

2 BACKGROUND OF STUDY

2.1 Cloud Computing: Background

2.1.1 What is cloud security?

The IT world has developed from mainframes to client computers, cloud computing, and the internet virtualization. Cloud computing offers a centralized repository of configurable IT service (e.g., computation, networking, applications, storage, and Information) on demand, as a distributed and versatile service, across a networked system, on a measured (pay-per-use or subscription) basis, which needs limited maintenance effort, is focused on service-level arrangements between the service provider and customers and is mostly used by the service provider and consumers. This also takes the form of internet-based tools or programs that users can view and use with a web interface as if it were a program installed locally on their personal computer (Abdul-Jabbar et. Al., 2020) .

Cloud computing can provide application (software-as-service), hardware (infrastructure-as-a-service) or technology tools (platform-as-a-service) that are accessible on request, to opposed licensed software and tools, or hardware purchases. The type and quality of operation and the specifications for cloud storage are, in most cases, decide upon in the Service Level Agreement (SLA) between the service provider and the customer (Alam, 2020).

2.1.2 Cloud role players.

Applications and other IT facilities are managed in-house in the conventional IT setting. Cloud computing provides applications, IT platforms, storage, or other resources in the cloud, somewhere within the bounds of the Internet. Services are offered by a third-party provider who hides the complexity of the underlying networks from the end customer.

Cloud computing building blocks are hardware and software architectures that allow infrastructure scaling and virtualization. Cloud computing architecture also involves cloud services (mediated services) offered by cloud service providers (vendors, third parties or brokers) to cloud customers (companies, IT staff or end users) over networked networks (i.e., Virtual private network or the Internet). These cloud storage services are regulated by contractual arrangements (SLAs) defining customer specifications and the obligation of the vendor to them (Sunyaev, 2020).

3 ARCHITECTURAL FRAMEWORK

Cloud computing combines different technologies to deliver effective services to end-users. In this section, the architectural framework of cloud computing is presented and shown in the figure 1. To understand the security issues of cloud computing, one of the most important things to understand is the framework and basic concept of what is involved in the cloud. In most literature, authors refer to the architecture of the cloud defined by the National Institute of Standards and Technology (NIST). The definition of cloud computing by the institute is widely accepted and used to offer a clear understanding of the cloud. According to NIST, these cloud models comprises of five (5) essential characteristics, three (3) cloud models and four (4) delivery models.

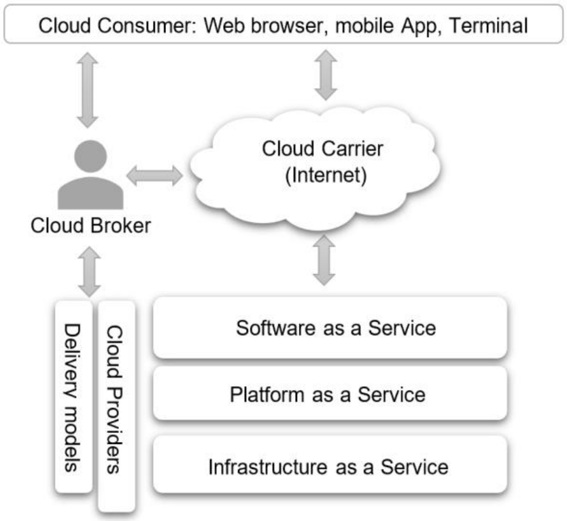

Figure 1 Architectural framework of Cloud Computing (Driesen & Eberlein, 2012)

3.1.1 Essential Characteristics

The five main characteristics of cloud computing provided by NIST includes:

I. On-demand self-service:

Using web services and management interfaces, consumers can make requests, manage access and services directly when needed. This can be achieved without any human interaction with service providers (Lee et. Al ., 2020)

II. Broad network access:

Cloud capabilities, data and services presented in the cloud network must be accessible using standard mechanisms that facilitate the use of heterogeneous systems for thin or thick client platforms (Herman et. Al., 2020). Devices like workstations, mobile phones, laptops etc. run with standard protocol and it is the nature of the cloud to support the protocols.

III. Resources Pooling:

The cloud providers provide large physical and virtual computing resources pooled and shared among multiple consumers. These resources are dynamically allocated according to the demands of the consumers, usually in a multi-tenant environment (Lee et. Al ., 2020).

IV. Rapid elasticity:

Capabilities, data, and services in the cloud can be elastically provisioned and released as it is a feature of the cloud to be elastic. These capabilities are scaled rapidly as per the demands of the consumers, in any quantity and at any given time.

V. Measured service:

The cloud system's metering functionality can be used to optimize and monitor services automatically according to customer demands. It is then possible to track the use of resources and report them to both the provider and the consumer. Where the consumers are charged in a pay-as-you-use manner (Lee et. Al ., 2020).

3.1.2 Service Models

The "SPI MODEL" is a generally accepted framework for defining the model of cloud computing services. The acronym “SPI” reflects the three cloud-based services model: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS):

I. Software as a service (SaaS):

SaaS is a capability provided to customers by a third-party provider to use its program, transfer data to remote storage on a cloud infrastructure. The programs are accessible from a variety of client devices through either a thin interface such as a browser or a program interface (Kavis, 2014). SaaS is typically available on demand to its customers. Salesforce, Oracle CRM, and Google Docs are well known examples of SaaS.

II. Platform-as-a-service (PaaS):

PaaS is a platform-oriented model with a higher-level programmable platform (Kavis, 2014). It provides a capability to customers to develop and deploy application onto the cloud infrastructure. The platform provides libraries, API's, programming models, IDE implemented and operated remotely for developing applications. Windows Azure, Google App Engine and RedHat OpenShift are examples of PaaS with an extensible environment.

III. Infrastructure-as-a-service (IaaS):

IaaS provides customers with essential computing tools to deploy and run arbitrary software's that could include operating systems and applications. It offers basic storage, virtualized infrastructure, and other abstract hardware and operating systems that can be managed by a service API (Velev, 2011). Examples of IaaS solutions are Amazon Web Service, Microsoft System Centre, and VMware vCloud Suite.

3.1.3 Deployment models

Regardless of the service model used, there are four key models in which cloud services can be implemented.

I. Private cloud:

The private cloud is managed and controlled internally by a single organization or by third party auditing (TPA). The private cloud model has a highly virtualized data centre located within the clients' firewall. It has unique workloads that offers a well-managed environment, efficient use of computing resources, protection, and compliance (S. Pal, 2011).

II. Community cloud:

Here, several organizations must share the same cloud infrastructure jointly with a particular group that has the same interest. Interest maybe requirements, services, security measures or applications.

III. Public cloud:

Public cloud is provided for free use by the public. It may be owned, controlled, and operated by, or a combination of a corporation, academic, or government entity. It resides at the cloud provider's premises.

IV. Hybrid cloud:

This cloud infrastructure is a combination of two or more cloud models. These infrastructures remain unique but are bound together by standardized or proprietary technology that enables portability of data and application.

3.1.4 Cloud roles and boundaries

The cloud has various predefined roles. NIST cloud computing architecture defines five main roles that are also known as actors. These actors (entities or organization) participate in processes or activities in the cloud infrastructure. This section explains the roles of each actor.

I. Cloud provider:

A cloud provider is referred to as a purveyor of cloud resources (Birje et. Al., 2017).The primary responsibility of the cloud provider is to make and ensure that the cloud services are available to the consumer.

II. Cloud consumer:

The cloud consumer is an entity or organization that consumes and uses cloud resources offered by the cloud providers (Birje et. Al., 2017).

III. Cloud broker

A cloud broker operates between the consumer and the cloud provider as an intermediary. The integration of resources can be too difficult for a customer to manage alone as the cloud infrastructure continues to evolve. Instead of a cloud provider, a consumer can request assistance from the broker to implement their desired services (Birje et. Al., 2017).

IV. Cloud carrier

The cloud carrier is a communication link, responsible for the transfer of data amongst all entities. In cloud computing, the internet serves as the carrier using the HTTP protocol to transfer information to/amongst various entities (Birje et. Al., 2017).

V. Cloud auditor

A cloud auditor is a third-party entity that carries out an independent examination on all cloud processes, controls, performances, and security threats with the intent to express an opinion on them (Birje et. Al., 2017).

4 CLOUD COMPUTING SECURITY

4.1.1 Security Issues in Cloud Computing

Cloud security is accomplished, in part, by third party controls and assurance, just as in conventional outsourcing arrangements. However, since there is no universal cloud computing security standard, there are additional problems associated with this. Often cloud services adopt their own proprietary protocols and encryption technologies and implement various security models that need to be judged on their own merits. In the cloud paradigm of the manufacturer, it is essentially up to the adoption of customer organizations, this is to ensure that protection in the cloud follows their own security policies by receiving specifications from the supplier. Danger evaluation, due diligence, and assurance practices (Singh & Chatterjee, 2017).

As a result, the security problems posed by companies seeking to employ cloud platforms are not fundamentally different from those relying on their own in-house controlled businesses. The same external and the same internal hazards are current and need risk control or acceptance of risks. In the following, we discuss the information management issues that companies will need to consider, either through vendor insurance or public cloud services, or specifically, through the creation and deployment of security measures in a privately held cloud. In specific, the following problems are examined:

- Treatment against information properties in cloud computing setting
- The forms of attackers and their ability to target the cloud

- The vulnerability threats involved with the cloud, and where applicable, the considerations of attacks and countermeasures
- Emerging vulnerability threats in the cloud
- A few examples of cloud protection accidents.

A. Components Affecting Cloud Security

Numerous security problems for cloud computing remain, including virtualization, space utilization, momentum management, cloud networks, concurrency control, memory management, operating systems, and database. For example, protection in a cloud network that interconnects devices in a cloud must be safe. The Cloud Computing Virtualization model results in a variety of security concerns (Ali & Vasilakos, 2015). And the mapping of a virtual machine to a real machine must be performed safely. Concurrency protection includes encrypting data as well as ensuring that acceptable protocols for data exchange are implemented. Resource allocation and memory management algorithms must be safe.

4.1.1.1 Security Issues Faced by Cloud Computing

Cloud makes it easy to reach the force of computation that beats. They have their own physical realm. It leads to a lot of security issues. The cloud service provider guarantees that the user does not face any issues such as data leakage or data theft. Cloud storage architecture uses emerging technologies and facilities, most of which have not been completely tested in terms of security. As a result, many users that share the contaminated cloud are affected. The security problems facing cloud computing are discussed below (Gupta & Gupta, 2014):

- **Data Access Control**: Often personal data may be obtained inappropriately due to a lack of safe data access control. Critical data in a cloud storage setting is emerging as significant security concerns in a cloud-based framework (Mondal et. Al., 2020).
- **Integrity of data**: Integrity of data involves situations where human error happens as data is entered. Errors may occur as data is transferred from one device to another, otherwise hardware malfunctions, such as disk crashes, may cause error (Mondal et. Al., 2020).
- **Data loss:** This is an important cloud computing problem. If banking and corporate transfers, research, and development concepts are all done online, unknown persons may be able to access shared knowledge (Mondal et. Al., 2020).
- **Administrative Access to Servers:** Consumer access to computing power is imperative is imperative to cloud service models. In data centres, access to servers with elevated privilege is restricted to on-site connections only. However, in cloud computing, access to servers with elevated privilege is done over the internet, making the infrastructure vulnerable to attack. Thus, it is crucial to restrict elevated privilege access and properly maintain access log for monitoring system control changes (Claywomb & Nicoll, 2012).
- **Privacy Issues:** User confidential information confidentiality is extremely critical for cloud computing. Many servers are external, so the provider can make sure that they are well protected from other operations (Mondal et. Al., 2020).
- **Data Theft:** Cloud Storage uses an online cost-effective and scalable data server for operations.
- **User level Issues:** user can guarantee that there is no lack of data or data tampering by those customers accessing the same cloud due to their own behaviour.
- **Security issues in Provider level:** Provider can allow a strong layer of security between customer and user. It should ensure that the server is well defended from any potential threats it will face.

4.1.2 Cloud Security Threats

In computer security terms, threats are circumstances that adversely impact the operations of a system. The 2020 cloud security report identified the biggest cloud computing threats as Misconfiguration of the cloud platform, unauthorized access, and insecure interface/API (Gautam & Jain, 2020). Other threats include Hijacking of accounts, External data sharing, and Malicious insider.

I. Side channel attacks:

The risk of side channel attacks which eventually leak data across multiple virtual machines in the same datacentre is a big issue for cloud delivery models that make use of virtualization technology (Zhang et. Al, 2016) . This allows attackers to act as customers to compromise other customers' data from within a shared cloud infrastructure.

II. Misconfiguration of cloud platforms:

According to the 2020 cloud security report by AWS, Misconfiguration of cloud platforms is the leading threat to cloud computing and a leading cause of data breaches. Customers outsource their software and data to the cloud, with the assurance that their assets are safe within the cloud environment. A minor misconfiguration can compromise the system's security, leaving the cloud resources exposed to attackers. Configurations must, as such, be well in place and compliant with security policies (Chaturvedi & Gupta, 2020).

III. Unauthorized Access:

Unauthorized access is another complex threat to deal with. Improper access control or misuse of employee credentials will make it possible for an intruder to obtain direct access, possibly without the knowledge of the organization. Improper access control in the sense that there are no appropriate access controls in place to avoid unauthorized access to the cloud infrastructure. The misuse of employees' credential, which is due to employee ignorance, as employees log in to the cloud infrastructure from various devices, i.e., home desktops, cell phones, or reusing passwords between company and personal accounts, or exchange passwords with colleagues to access accounts. All this leaves the device vulnerable to external threats (Chaturvedi & Gupta, 2020).

IV. Insecure interface/API:

To access and communicate with cloud services, cloud service providers expose clients with a set of APIs and software interfaces. The management, monitoring and provisioning of the cloud services is provided by these interfaces. As such, the security and availability of the general cloud services depends on the security of these fundamental (Chaturvedi & Gupta, 2020). These interfaces, however, must be configured to protect against accidental as well as malicious attempts to disrupt the protection of these APIs. Weak interface/APIs can expose clients to various security threats, such as sensitive data leakage, anonymous access, restricted monitoring, modification of application configuration settings, etc.

V. Hijacking of Accounts:

Account or service hijacking is done using compromised customer credentials to gain access to the cloud services. This can be executed through phishing or manipulation of vulnerabilities in software. The reuse of credentials often contributes to such attacks in some situations. With the compromised credentials, the attackers can gain access to sensitive parts of the cloud services compromising confidentiality, integrity, and availability of the services (Alam, 2020).

VI. External Data-Sharing:

Data sharing has become a vital operation for almost every organization. The cloud system was built to make data sharing a lot easier. Using cloud, collaborators can easily be invited via emails or a shared link that enables anyone with the URL to access and adjust the shared resource. While this easy exchange of data is considered an asset, the link may be shared, stolen, or guessed, providing unauthorized access to the resources. This could undermine the confidentiality and integrity of the shared resources (Alam, 2020). Also, once this connection is shared, access to the recipient cannot be revoked.

VII. Malicious Insider:

This challenge is a big security concern that is difficult to protect against. It involves an insider who can easily access a system's critical resources or control over the cloud services at higher levels with little or no risk of detection. A malicious insider's actions adversely affect the confidentiality, integrity, and availability of information and has an impact on internal activities, company reputation, and customer trust (Alam, 2020).

4.1.3 Cloud Security Attacks

I. Denial of service attacks:

DoS attack is when an attacker sends thousands of requests to exhaust all the resources the server has until it becomes unavailable. The request packet wastes the capacity, cryptographic operations, and performance time. This affects the clouds behaviour and availability (Mittal, 2020). Compared to a DoS attack, a distributed DoS attack is much more complicated and harder to detect.

II. Man-in-the-Middle attacks:

A man in the middle attack refers to an attack where a malicious actor secretly inserts him/herself between two communicating parties to obtain access to information being exchanged or, possibly alter the data that is been sent and received across without the knowledge of both parties (Jansen, 2020). This attack is possible only if the communication channels are not secured or lack security configurations in the Secure Socket Layer (SSL) (Jansen, 2020).

III. Phishing Attacks:

Phishing attack is a type of social engineering technique that uses disguised email as a weapon. It occurs when an attacker masquerades a legitimate entity with a link or an attachment, creating a sense of urgency and curiosity (Mondal & Goswami, 2020). When a user clicks on the link, he/she is redirected to a fake website without their knowledge and are asked to enter their login credentials. When the user enters the credentials, the attacker can gain access to it.

5 EXISTING SECURITY SOLUTIONS

5.1 Existing Solutions

- Intrusion Detection and Prevention - Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) safeguards enterprise applications and operating systems vulnerabilities till a patch or an update is made available, to prevent attacks like Zero-day attack. VMs and Cloud servers often use similar system software, application software and physical infrastructure. However, software-based IDS and IPS deployment on VMs safeguards protects against vulnerabilities (Negi et. Al., 2020).

- Firewall - A firewall can be used to reduce the attack surface of VMs in a typical cloud environment. A two-way firewall or bi-directional firewall is deployed on specific VMs, while providing an integrated management of firewall policy (Li et. Al., 2020). However, the firewall policy should include and enable the following templates: 1. VM separation 2. Fine-grained filtering 3. Coverage of all frame types and IP-based protocols 4. Ability to create policies for each network interface.

- Log Inspection - Log Inspection and analysis of logs from operating system and application logs for security related events. Log Inspection rules allow for the optimization of security event detection, usually events lost in multiple log entries (Negi et. Al., 2020). A Security Information and Event Management (SIEM) system ensures maximum visibility of events received. However, a cloud-based log inspection software allows for the following: 1. Collation of security related actions. 2. Detection of suspicious activity. 3. A collation of security related events across the server farm.

5.1.1 Recommendations

These recommendations are targeted towards cloud service providers and consumers. While considering human factors in security, malicious actors have resorted to more advanced ways of gaining access into protected networks and applications. However, users should always be wary of malware threats whilst surfing the internet and use a carefully phrased strings of credentials for different applications. Additionally, applications should enforce a password policy whereby common phrases or strings of password are unacceptable. According to Goodin (2012), the more complex a password is, in terms of length, drastically increases the time taken to crack the password, eventually addressing the risk of brute-force cracking. The

Secure Hash Algorithm-1 (SHA-1) and the Message Digest 5 (MD5) both have a design goal of being fast and whilst making use of very minimal computing resource. This goal reduces the efficacy of brute-force attacks, and a single iteration of crypto hash function is not sufficient to store salted passwords. However, it is recommended to utilize slower and multi-iteration hashing algorithms like bcrypt (Kamal, 2019). This approach may considerably reduce of brute-force cracking methods in cloud computing, but the computational requirements will increase. Hence, it is left to cloud service providers to wisely deem between the security level and performance.

Another recommendation is for cloud service providers to enforce Two-Factor Authentication (2FA), as most cloud service providers like Google and Apple have done. This is motivated by security intrusion and weak password choices by consumers (Mohsin et. Al., 2017). The Two-Factor Authentication builds upon the existing login process of provides user ids and passwords by adding a securely generated and delivered token. This token is a time-based access code which is usually refreshed periodically, establishing the One-Time-Password (OTP). Similarly, the authentication server runs a time-based algorithm as the initial pre-shared key to generate synchronized codes with the token. This is requested by the login system after the provision of user ids and passwords (Kumar et. Al., 2020).

A systemic, yet prudent examination of cloud deployment models should be considered in creating a balanced merit to demerit ratio whilst focusing on the security aspect. In that case, licensed and trusted 3rd party auditors may be called upon. However, to avoid attacks, cloud service providers should close OpenDNS resolvers and consider security as the topmost priority. Security should be deployed in both hardware and software and be implemented in all parts of the Software Development Life Cycle (Sen & Madria, 2020).

5.2 Conclusion

Cloud computing has emerged significantly within the past decade, with major innovations and advances adopted widely in various industries due to a more practical service and convenience. Enterprise and Organization reap benefits from adopting cloud solutions within their businesses. However, cloud security is a vital part of computer security, this poses a challenge because of the extensive adoption of cloud computing and the internet connection aspect of cloud computing makes the service vulnerable to various types of security threats. The significant threats to cloud security are extensively reviewed in this paper. Additionally, countermeasures and threat mitigation solutions are offered to serve as recommendations. Similarly, the comprehension of issues faced by cloud security and workable solutions is vital to diminishing the risks associated to cloud computing adoption.

6 REFERENCES

1. Abdul-Jabbar, S.S., Aldujaili, A., Mohammed, S.G. and Saeed, H.S., 2020. Integrity and Security in Cloud Computing Environment: A Review. *Journal of Southwest Jiaotong University*, *55*(1).
2. Alam, T., 2020. Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), pp.108-115.
3. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences (Ny)*, *305*, 357–383.Claycomb, W.R. and Nicoll, A., 2012, July. Insider threats to cloud computing: Directions for new research challenges. In 2012 IEEE 36th Annual Computer Software and Applications Conference (pp. 387-394). IEEE.
4. Birje, M.N., Challagidad, P.S., Goudar, R.H. and Tapale, M.T., 2017. Cloud computing review: concepts, technology, challenges, and security. *International Journal of Cloud Computing*, *6*(1), pp.32-57.
5. Chaturvedi, C. and Gupta, B.B., 2020. Cloud Computing Security: Taxonomy of Issues, Challenges, Case Studies, and Solutions. In *Handbook of Research on Intrusion Detection Systems* (pp. 306-325). IGI Global.
6. D. Velev and P. Zlateva, "Cloud Infrastructure Security", *Lecture Notes in Computer Science*, pp. 140-148,2011. Available: https://www.researchgate.net/publication/220865671_Cloud_Infrastructure_Security. [Accessed 2 November 2020].
7. Driesen, V. and Eberlein, P., SAP SE, 2012. Brokered cloud computing architecture. U.S. Patent 8,250,135.
8. Gautam, R. and Jain, M., 2020. Cloud Computing Security: Aws Data Security Credentials. *Studies in Indian Place Names*, *40*(3), pp.6385-6389.
9. Goodin, D., 2012. Why passwords have never been weaker-and crackers have never been stronger. *Ars Technica*.
10. H. Gupta and D. Kumar, "Security Threats in Cloud Computing", *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, 2019. Available: https://ieeexplore.ieee.org/document/9065542. [Accessed 26 December 2020].
11. H. Schulze, "AWS Cloud Security Report 2020 for | Cloud Security Alliance", *Cloud Security Alliance*, 2020. [Online]. Available: https://cloudsecurityalliance.org/blog/2020/10/14/aws-cloud-security-report-2020-for-management-managing-the-rapid-shift-to-cloud/. [Accessed 28 December 2020].
12. Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., Lee, R., Landreville, N.M., Mishra, A.K., Wang, Y. and Sardinas, R., 2020. *NIST Cloud Computing Forensic Science Challenges* (No. NIST Internal or Interagency Report (NISTIR) 8006). National Institute of Standards and Technology.

13. Jansen, L.W.L., Comparing cloud security directions between the academia and the Industry, A survey.
14. Kamal, P., 2019. Security of Password Hashing in Cloud. *Journal of Information Security*, *10*(02), p.45.
15. Kavis, M.J., 2014. *Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS)*. John Wiley & Sons.
16. Kumar, S., Jafri, S.A.A., Nigam, N., Gupta, N., Gupta, G., and Singh, S.K., 2020, February. A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing. In *IOP Conference Series: Materials Science and Engineering* (Vol. 748, No. 1, p. 012026). IOP Publishing Ltd.
17. Lee, C.A., Bohn, R.B., Michel, M., Delaitre, A., Stivalet, B., Black, P.E., Okun, V., Ribeiro, A., Cohen, T.S., Libert, J. and Grantham, J., 2020. The NIST Cloud Federation Reference Architecture 5. *NIST Special Publication*, *500*, p.332.
18. Li, J., Jiang, H., Jiang, W., Wu, J. and Du, W., 2020, May. SDN-based Stateful Firewall for Cloud. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)* (pp. 157-161). IEEE.
19. Mittal, R., 2020, October. Analysis of DDoS Attacks in Cloud. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 19-23). IEEE.
20. Mohsin, J.K., Han, L., Hammoudeh, M. and Hegarty, R., 2017, July. Two factor vs multi-factor, an authentication battle in mobile cloud computing environments. In *Proceedings of the International Conference on Future Networks and Distributed Systems* (pp. 1-10).
21. Mondal, A. and Goswami, R.T., 2020. ENHANCED HONEYPOT CRYPTOGRAPHIC SCHEME AND PRIVACY PRESERVATION FOR AN EFFECTIVE PREDICTION IN CLOUD SECURITY. *Microprocessors and Microsystems*, p.103719.
22. Mondal, A., Paul, S., Goswami, R.T. and Nath, S., 2020, January. Cloud computing security issues & challenges: A Review. In *2020 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-5). IEEE.
23. Negi, P.S., Garg, A. and Lal, R., 2020, January. Intrusion Detection and Prevention using Honeypot Network for Cloud Security. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 129-132). IEEE.
24. S. Gupta and P. Gupta, "A Study of the Issues and Security of Cloud Computing", *International Journal of Computer Science and Information Technologies*, vol. 5, pp. 5432-5433, 2014. [Accessed 28 December 2020].
25. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey", *Journal of Network and Computer Applications*, vol. 79, pp. 88-115, 2017. Available: 10.1016/j.jnca.2016.11.027 [Accessed 26 December 2020].
26. Sunyaev, A., 2020. Cloud Computing. In *Internet Computing* (pp. 195-236). Springer, Cham.
27. T. Yu and Y. Zhu, "Research on Cloud Computing and Security", *2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science*, 2012. Available: https://ieeexplore.ieee.org/document/6385297. [Accessed 28 December 2020].
28. Zhang, D., Jiang, T. and Wu, S., 2020. Brief Talk on Cloud Computing Technology. *International Journal of Social Science and Education Research*, *3*(6), pp.168-171.