LAFIA JOURNAL OF LIBRARY AND INFORMATION SCIENCE
Volume 2, Number 1, 2022.
https://lalibjournals.org/index.php/LJLIS
ISSN: Print - 2814-0702, Online - 2814-0710
LJLIS

DATA STORAGE IN THE CLOUD: A HISTORICAL PERSPECTIVE

Ekhaguosa, Vincent Osamuyimen
Igbinedion University Library, Okada,
Edo State, Nigeria.

Omorogbe, Harry Osasu
Igbinedion University Library, Okada,
Edo State, Nigeria. State, Nigeria.

Abdulsalami, Lucky Tijani Ph.D
Igbinedion University Library, Okada,
Edo State, Nigeria.

Abstract
The study sought to establish cloud computing and Data storage learning on the integration of computer technology into the future. The focus of the study is on the security of data storage from cloud computing, providing users with insight into the security of data storage in the cloud. When cloud computing was new, questions spun around the ability of cloud service providers to keep their infrastructure secure. As more businesses began migrating to the cloud, it became obvious that the major cloud service providers were better fortified than most organizations to secure their networks, and customers of cloud services continue to seek better ways to secure their data. Currently, cloud security is becoming less of a distinct exercise and more of a primary element of overall security and data protection strategies, cloud is so universal that securing cloud applications and data is itself among the top priorities, and much of the responsibility for securing cloud applications and data has fallen on the organizations using cloud services. To educate people about cloud computing and data storage security, cloud computing, cloud storage, cloud security, benefits of cloud computing, cloud data storage: (security, protection, and privacy), cloud services are part of our daily life, and when you enter the world of work, this interaction will only increase. Learning how cloud storage works today and how to protect yourself from its dangers will help you become a smarter and safer consumer as cloud technologies continue to evolve.

Keywords: Cloud computing, cloud storage, data storage, cloud security, data, cloud applications

Introduction

Currently, the sale of digital devices (smartphones, Android, and tablets) has exploded. With these mobile devices, users can access their data and applications anywhere, anytime, as long as the internet is available. The traditional Information Technology (IT) infrastructure is no longer suitable for universal access to data. It becomes expensive and difficult to manage. The swift increase in global internet usage requires a new way to manage the size, variety, and availability of data, which is Cloud Computing. Cloud Computing introduces a new way of providing resources to users as a service accessible via the Internet. Unlike the old-fashioned approach that is based on hardware ownership where data is stored, Cloud Computing users no longer own the infrastructure that is controlled by these service providers. The transmission of infrastructure control to the service providers involves the transmission duty associated with data security. The Cloud Computing domain is so wide that it is unmanageable to deal with all of its aspects. This paper focuses on aspects related to Cloud Computing storage, and more particularly, we are interested in the safety of data storage hosted on the Cloud. Technology development and advancements have always had important impacts on education.

The pressure to deliver good services from very insignificant resources has overwhelmed learning institutions all over the world. Cloud computing plays a major role in improving the quality of education to attain high performance by offering many benefits for education such as flexibility, scalability, providing infrastructure with low cost, collaboration, flexibility, and ease of use. Furthermore, it allows users to store and access data on-demand from anywhere via the internet (Al-Shqeerat, Hammoudeh, & Abbasm, 2016). The cloud services and applications enable users to store and access their local data in the remote data center by using their personal computers, or mobile devices (Raoa & Selvamanib, 2015). Cloud Computing offers on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, and services, rapidly provisioned with minimal management effort and provider interaction (Cachin, 2011). Infrastructure as a service (IaaS), Software as a service (SaaS), Platform as a Service (PaaS), Storage as a Service, and recently, Security as a Service (SECaaS), etc in a multi-tenant model at relatively low cost, and high resource availability over fast Internet connectivity. Storage as a Service is generally seen as a good alternative for a small or mid-sized business that lacks the

capital budget and/or technical personnel to implement and maintain its storage infrastructure. SaaS is also being promoted as a way for all businesses to mitigate risks in disaster recovery, provide long-term retention for records, and enhance both business continuity and availability.

Purpose of Study

1. The security of data storage in cloud computing gives users' insight into the security of data storage in the cloud.
2. Educate people about cloud computing and data storage security

Review of Related Literature

According to NIST (2012), Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Depending on the type of capacity provided, there are four scenarios in which the cloud is used, as shown in Figure 1.1.

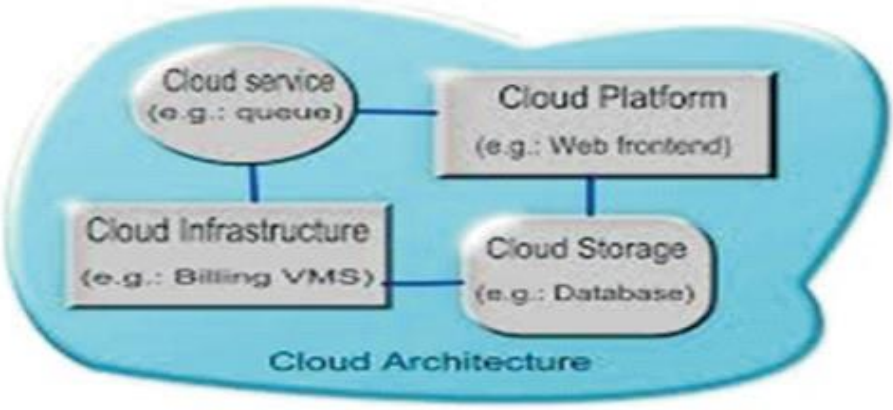


Fig. 1.1

This cloud model is composed of five essential characteristics, three service models, and four deployment models" (Sivakumar & Singaravelu, 2016), According to Kaushik and Kumar (2013), two models are working for cloud computing which are Deployment Models and Service Models. Cloud Deployment Models: Deployment models define the types of access to the cloud i.e. how the cloud is located. Cloud can have any of the four types of access- 1) Public Cloud. 2). Private Cloud. 3). Hybrid Cloud. 4) and Community Cloud while

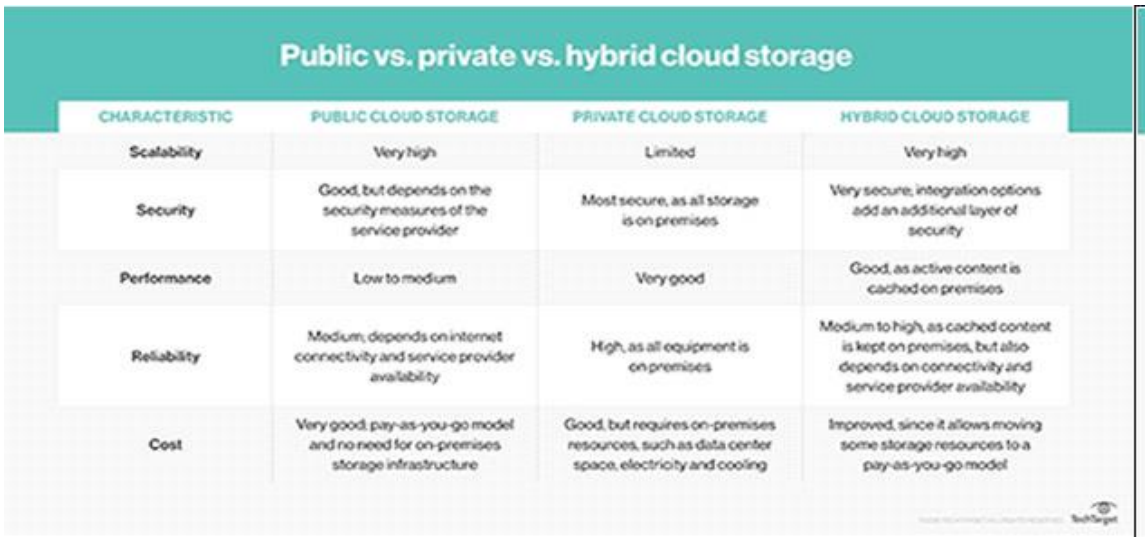
Cloud Service models: are- (1) Infrastructure as a service (IaaS) (2) Platform as a Service (PaaS) (3) and Software as a Service (SaaS). Service Description model: Software as a Service (SaaS). SaaS facilitates promotes user entry to applications and databases. The user does not have to install and run the app on their local computer. Maintenance is simple in SaaS, so it is quite cost-effective (Irfan et al., 2015). Platform as a Service (PaaS). PaaS model, provides you with infrastructure as well as full operating and developing ecosystems to deploy your applications (Goyal, 2014). Infrastructure as a Service (laaS). The capability provided to the consumer is to make provision for processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. (Ekhaguosa et al, 2022). Storage as a Service (StaaS), it enables cloud applications to expand beyond their limited servers. StaaS allows users to store data on remote disks and access it anytime, anywhere. Cloud storage systems must meet several stringent requirements to preserve user data and information, including availability, reliability and performance, replication, and data consistency. However, due to the inconsistent nature of these requirements, no system will implement them all together.

Cloud Storage

Chai, Castagna, & Lelii, (2021) defines Cloud storage as a service model in which data is transmitted and stored on remote storage systems, where it is maintained, managed, backed up and made available to users over a network, typically, the internet users generally pay for their cloud data storage on a per-consumption, monthly rate. Cloud storage is based on a virtualized storage infrastructure with accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud-based data is stored in logical pools across disparate, commodity storage servers located on premises or in a data center managed by a third-party cloud provider. Cloud service providers manage and maintain data transferred to the cloud. Storage services are provided on demand in the cloud, with capacity increasing and decreasing as needed. Organizations opting for cloud storage eliminate the need to buy, manage and maintain in-house storage infrastructure. Cloud storage has radically driven down the per-gigabyte cost of storage, but cloud storage providers have added operating expenses that can make the technology considerably more expensive, depending on how it's used. (Chai, Castagna, & Lelii, 2021))

There are three general types of cloud storage: private cloud storage, public cloud storage, and hybrid cloud storage. Public cloud services are defined by

being accessible through the internet to customers from a third-party service provider (Irfan et al., 2015). Public cloud is available to government use, and it is a cost-effective solution for applications hosting. There are few instances: Google, Amazon and Microsoft. A private cloud is hosted in a company's data centre and offers its facilities only to users within that firm or its associates (Goyal, 2014). Hybrid cloud utilises both government and private cloud methods where it relates the strategy views of public cloud services with the private cloud foundation. In reality, the private cloud must be connected to the rest of the company's IT resources and cannot be separated from the public cloud (Alzahrani, Alalwan & Sarrab, 2014).



Public vs. private vs. hybrid cloud storage

CHARACTERISTIC	PUBLIC CLOUD STORAGE	PRIVATE CLOUD STORAGE	HYBRID CLOUD STORAGE
Scalability	Very high	Limited	Very high
Security	Good, but depends on the security measures of the service provider	Most secure, as all storage is on premises	Very secure, integration options add an additional layer of security
Performance	Low to medium	Very good	Good, as active content is cached on premises
Reliability	Medium, depends on internet connectivity and service provider availability	High, as all equipment is on premises	Medium to high, as cached content is kept on premises, but also depends on connectivity and service provider availability
Cost	Very good, pay-as-you-go model and no need for on-premises storage infrastructure	Good, but requires on-premises resources, such as data center space, electricity and cooling	Improved, since it allows moving some storage resources to a pay-as-you-go model

Table 1: Adopted from TechTarget Network 2021

Security Vulnerabilities in Mobility and Cloud Government Applications

Despite the growing use of mobile computing, unique challenges such as secure resources, frequent disconnections, and mobility make it difficult to fully utilize its potential benefits (Fernando, Luque, & Rahio, 2013). Data in the cloud is usually in a shared environment with other customers' data. Encryption is important to protect data confidentiality and data privacy during transmission and cloud storage. Legally, third-party cloud service providers (CSPs) and their customer organizations are separate companies. Failure of the CSP to fulfill its responsibilities may result in legal consequences for the CSP's client organization. In contrast, if a cloud customer organization fails in its responsibilities, it is less likely to be exposed to legal implications of the CSP (LLP, Chan, Leung, & Pili,

2012). There are some responsibilities for the organizations such as flexibility access issues of cloud providers, protect sensitive data in the cloud computing, understanding legally and standards issues, software development life cycle management, portability and interoperability, and cloud platform reliability and latency. Open Security Architecture (OSA) provides frameworks that are easily integrated into software applications for the security architecture community. Its patterns are based on schematics that show the data traffic flow control for secure cloud computing and particular implementation with policies implemented at each step for the cloud security issues. The cloud mobile applications can connect and request services hosted on remote cloud computing by interfaces (Al-anzi, Yadav, & Soni, 2014). However, mobile Web services need to consider additional constraints other than standard Web services: frequent loss of connectivity, low computational resources, and low bandwidth (Carroll, Merwe, & Kotze, 2011).

Cloud Security Services and Application Issues

Service and application level issues related to the security factors concerned with performance measurements of the cloud computing system, and the quality of service and cloud service level agreement (Rolim, Koch, Westphall, Werner, Fracalossi, & Salvador, 2010). Therefore, a cloud of services can extend dynamically to meet user-on-demand requirements. Cloud security data typically, data in cloud computing is owned by multiple owners of trusted cloud computing resources. Therefore, unauthorized users should reject such data or information (Rohmeyer, & Ben-zvi, 2015). In trusted data and cloud data, confidentiality refers to the original data that must be protected and password-protected by a data management system through a security service in a cloud computing environment. All cloud data are entered, stored, and backed up in a password protected by the management of data in cloud computing (Al-Attab & Fadewar, 2014). Besides, the data storage is a model of data storage in which the integrity data is stored in logical pools. It allows cloud users to store their data in a remote server to get rid of expensive local storage and manage brand costs and then the flexibility to access data of interest anytime and anywhere (Dinh, Lee, Niyato, & Wang, 2013).

Cloud Security Services and Application Issues

Service and application level issues related to the security factors concerned with performance measurements of the cloud computing system, and the quality of service and cloud service level agreement (Rolim, Koch, Westphall, Werner, Fracalossi, & Salvador, 2010). For example, in what ways do mobile cloud computing systems ensure data of availability; what are the fault-tolerance (FT)

mechanisms employed to ensure smooth execution and uninterrupted service (Sengar, 2015) Therefore, a cloud of services can extend dynamically to meet user-on-demand and requirements. Additionally, the capabilities of the cloud can be rapidly and elastically increased to meet immediate demand and scaled down to release unused resources. However, monitoring should be done by the cloud service provider frequently to ensure that the cloud is secure and not infected by the malicious code that has been uploaded to the cloud by hackers or attackers to steal sensitive data or even damage the information of users.

Cloud Security Data Issues

Generally, the data in cloud computing belongs to different owners in the cloud computing resources which must be trusted. Therefore, unauthorized users should be forbidden from that data or information (Rohmeyer, & Ben-zvi, 2015). In trusted and sensitive cloud data, confidentiality refers to the original data that must be kept with a password by data management systems with security services in cloud computing environments. All cloud data is captured, stored, and backed up in a password-protected data manager in Cloud Computing (Al-Attab & Fadewar, 2014). Cloud data storage is also a data storage model in which integration data is stored in logical groups. It enables cloud users to store their data on a remote server to eliminate expensive local storage and manage branding costs and thus the flexibility to access critical data anytime, anywhere (Dinh, Lee, Niyato, and Wang, 2013).

Cloud Security Network Issues

Cloud security is a network security issue. Cloud computing allows constant, convenient, and on-demand access to a shared network of configurable networks that can be quickly provisioned and shared without administrative effort or communication with service providers (Soufi & Khan, 2014). Because cloud computing implements a relatively new computing model, there is significant uncertainty about how to achieve network security and improve application security for cloud computing (Kaashyap & Sarika, 2015). The problem of the cloud network is the response time of most nodes when communicating data over shared storage.

Cloud Security Platform and Infrastructure Issues

Cloud infrastructure security depends on the cloud and trusted encryption. Additionally, there is no standard service contract that covers the range of cloud services available and the needs of different organizations. Besides that the cloud

computing technology allows to design and implemented a real-time alert system on top of the cloud infrastructure (Sasikaladevi, 2016). However, cloud computing offers an elastic infrastructure that Cloud Management Agents can use to obtain streaming resources that match the demand. Also, multi-cloud providers support different platforms and offer constantly changing packages of capabilities. Cloud infrastructure security issues are the risk associated with users' concerns and are also the focus of this work's research direction. Therefore, the centralized security solution for the insecure cloud is proposed and the scenarios of this system and procedures are made.

Factors behind Cloud Vulnerabilities

Many cloud vulnerabilities can be caused by a variety of technologies, including networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency monitoring, and memory management used in cloud computing. In addition, cloud computing is designed as a computing service. Customers rent cloud computing resources to get their work done. Therefore, to ensure customer-defined Quality of Service (QoS) requirements and ensure resource utilization in cloud data centers, effective resource management systems must be considered. Therefore, with more individuals and enterprises migrating their work into the cloud, workloads in the cloud become more heterogeneous. Meanwhile, cloud computing resources are much more heterogeneous as cloud providers constantly scale or update the clusters with new generations of machines (Xu & Li, 2016). However, in reality, government organizations run applications and data transfers in their private cloud and then transmute it to the public cloud. While many security issues exist in cloud computing technology, cloud security should design relevant standards and policies as soon as possible (Bouchenak, Gheorghe, Chockler, Chockler, & Shraer, 2013).

However, cloud computing is changing the current IT delivery model for services. Benefits for business and IT include reduced costs, scalability, flexibility access to data on cloud storage, capacity utilization, higher efficiencies, performance, and mobility (Rajaei & Wappelhorst, 2011). Generally, cloud computing's issues can bring negative effects on any company or organization, therefore effective risk management is needed to balance the operational and financial costs as well as proactive actions to secure data, network, platform information systems, and technologies (Al-shargabi & Sabri, 2016). According to Meena, Devi and Priya, (2016), understanding the true potential of mobile cloud computing and identifying mobile cloud security, privacy, feasibility, and

accessibility issues remain of great interest to customers and businesses (Ahmed & Abraham, 2013). Therefore, cloud security issues and their existence have a significant impact on the success of cloud computing systems. Cloud security, cloud data privacy, feasibility, and accessibility remain concerns for users and businesses (Srivastava, & Sudhish, 2015). The cloud environment has major cloud security issues (Al-Musawi, Al-Badi & Ali, 2015). Improper key storage can lead to data encryption. Flexibility in accessing the key data store should be limited to authorized personnel who require separate keys. These keys should be subject to guidelines (Saranya, Ramya, Kumar & Nalini, 2016).

Discussion of Data Storage in the Cloud

Storing Data in the Cloud: (Safety, Security, and Privacy). Every sector of the economy is on the verge of living almost completely wirelessly, and that goes well beyond our tablets and phones. For a long time now, information has been rapidly leaving the physical, paper-bound world and setting up shop in the digital atmosphere, tethered to us with invisible strings. For all of the progress that has been made to bring technology to the forefront of information storage, one method, cloud storage, is the subject of a great deal of controversy and speculation despite its daily use. The need to have your information and storage on the go is vital for every college student, and to that end, cloud storage cannot be beaten. You may already be using cloud-based apps like Google Drive, Dropbox, and Apple iCloud. College hybrid classes are also becoming the norm, and it's hard to imagine a world where your music is not protected. Instagram, YouTube, and Snapchat all use the cloud. When it comes to the security features available on these platforms, you will be hard-pressed to find anything better.

How Cloud Storage Works. It all starts with data centers, tremendous buildings filled with nothing but networked computers, which you access over the internet. These centers house servers, which create the infrastructure for cloud-based systems. There are a lot of other terms that you may have heard about, like "elasticity" or "redundancy," but essentially, the cloud is all about another term, "virtualization." effectively entails several operating and maintaining values, which implies that many businesses are unable to spend in new fields (Suzuki and Juli, 2017). This allows a single machine and interface to be used by potentially millions of people at the same time across the cloud.

Currently, there are more than 50 million servers around the world supporting all of those seamless features of cloud apps. All of your information including your photos, your English Lit papers, and your credit card account, are

stored at dispersed data centers around the world.. For example, when you log into Gmail, it does not matter if you are logged in from your phone or tablet or visiting your parents' laptop. All your information is delivered to you in the same format every time.

Data Security: All of these centers have living individuals who are responsible for protecting and accessing your data. Cloud providers work to give you the best value for what you pay, and they often store backups of encrypted information in additional data centers. These companies are responsible for data breaches, but it's up to you about what information you can trust. Encryption is the key to giving only you access to your data, and that's what you as a customer suffer. While your company and your cloud storage company are working to provide encryption on their side, it is still up to you to protect yourself from potential harm. In the end, your safety is your responsibility. (Soofi, & Khan, 2014)

Privacy in the Cloud: While businesses are required to ensure that they do not unintentionally give out their employee's personal information when using cloud storage, your privacy is wholly dependent on how much information you are willing to share over the internet. That sharing includes backing up your phone and photos too, so just because you haven't shared it publically does not mean that you're not sharing personal info with cloud storage companies. Tax information, personal identification information, and sensitive materials should never be stored in the cloud, no matter the level of security in place. The future of cloud storage may one day provide the necessary means of protecting this vital data, but currently, they do not.

Pins, fingerprint identification, dual-step security features, and strong, hard-to-guess passwords are all methods of encryption that you, the customer, provide. First, be sure that you are choosing passwords and pins that are not used for anything else. If your usernames and passwords are the same for more than one login, you are putting your information at risk unnecessarily. Second, by adding additional login steps to your accounts, you make sure you add layers of protection that can help cloud-based applications. Third, you do not need to store absolutely everything in cloud storage. When it comes to disclosing your personal information, including your social security number, credit card information, and other information that identity thieves can steal, you can and should choose a personal hard drive such as a hard drive or folder encrypted on your computer. Just as data breaches are reported in many different companies, it has also been reported that very often it is user error that puts information at risk. Take, for

example, the massive celebrity photo leak a few years ago. It was not just the cloud data center that accessed these photos. It was also the celebrity's fault that made it easier for thieves to hack into a private cloud because they didn't properly protect their information. We are used to living in a world of comfort and accessibility, but we are not free to do so. The price of staying wirelessly connected to any Internet application is that you have to spend time and energy protecting yourself. Cloud storage is essential to our digital infrastructure, it's needed to realize how we want to live and it's good at it, but not everything is reliable. As technology advances and encryption methods become more effective, data will be protected in ways that have yet to be discovered. Until that day comes, however, be sure that you take your security into your own hands and create the safest possible form of cloud storage to fit your needs.

Conclusion

There are factors helping to keep data secure in a cloud platform.

1. **Redundancy**: Losing data can be almost as harmful as having it stolen. When a server fails or a hacker gains access to a corporate network and deletes or attempts to ransom vital information, companies can lose months of productivity. Most cloud networks, however, typically keep data in at least three locations. This means that data loss in one location, such as data loss due to a server failure, will not have the devastating impact it can have on an organization that depends on a local data center. By keeping copies of every file, cloud solutions ensure that business-critical data is available until the user no longer wants it.
2. **Secure sharing policy**: who has ever use Google Docs knows how file sharing works. Instead of copying, the user must enter the email address of anyone who wants to see the file. These additional users cannot share the file themselves unless explicitly allowed,they simply have access to the information. Here is how secure sharing works. Prevent the creation or distribution of unauthorized copies. Users can access their data and control exactly who sees it.
3. **Encryption**: If you keep track of your passwords, it will be very difficult for hackers to access your files. They are stored entirely in the cloud or secure in remote facilities in unknown locations. Since the user's communication with this information is encrypted, it would be difficult, if not impossible, for a human hacker to track it down for access.

The Way Forward

Cloud services are a part of our regular daily lives, and as you enter the workforce, that interaction will only increase. Learning how cloud storage works

now and how to protect yourself from its dangers of it will serve to make you a smarter and safer consumer as cloud technologies continue to evolve.

References

Ahmed, N., & Abraham, A. (2013). Modeling Security Risk Factors in a Cloud Computing Environment. *In Folklore Forum*.

Al-anzi, F., Yadav, S.& Soni, J. (2014) Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance, in 2014 *International Conference on Data Mining and Intelligent Computing (ICDMIC)*, 1–6

Al-Attab, B. S. & Fadewar, H. S. (2014) Security Issues and Challenges in Cloud Computing. *The International Journal of Emerging Science and Engineering (IJESE)* 2(7), 22–26.

Alzahrani, A., Alalwan, N. & Sarrab, M. (2014) Mobile Cloud Computing: Advantage, Disadvantage and Open Challenge, *Proceedings of the 7th Euro American Conference on Telematics and Information Systems*, 4–7

Al-Musawi, F., Al-Badi, A. H., & Ali, S. (2015, September). A road map to risk management framework for successful implementation of Cloud Computing in Oman. *In 2015 International Conference on Intelligent Networking and Collaborative Systems* (417-422). IEEE.

Al-shargabi, B., & Sabri, O., (2016) A study of Adopting Cloud Computing from Enterprise.

Al-Shqeerat, K. H. A., Hammoudeh M. Ali A., & Abbasi. M. I., (2016). Design and Analysis of an Effective Secure Cloud System at Qassim University. *International Journal of Computer Science and Information Security (IJCSIS)*. 14 (8).

Bouchenak, S., Gheorghe, G. Chockler, G., Chockler, H., & Shraer, A., (2013) Verifying Cloud Services: Present and Future, Association of Computing Machinery SIGOPS *Operating System*. Reviewed 27(2). 6 – 19,

Cachin, C. (2011) Protocols for Secure Cloud Computing, *IBM Corporation Research* – Zurich metis2011.pdf (cachin.com)

Chai, W., Castagna, R., & Lelii, S., (2021) cloud storage *techtargetNetwork* https://www.techtarget.com/searchstorage/definition/cloud-storage retrieved 15th July 2022

Chan, W., Leung, E. & Pili, H. (2012) Enterprise Risk Management for Cloud Computing. *The Committee of Sponsoring Organizations of the Treadway Commission* (COSO), Chicago. http://www.coso.org/documents/ Cloud%20Computing%20Thought%20Paper.pdf

Carroll, M., Merwe, A. Van Der & Kotzé, P. (2011) Secure Cloud Computing

Benefits, Risks, and Controls. *Information Security South Africa (ISSA*), Johannesburg, 15-17 August, 1-9.

Dinh, H. T., Lee, C., Niyato, D., & Wang, P., (2013) A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches, *Wireless. Communication and Mobile Computing*. 13(18), 1–38

Ekhaguosa, V. O., Otote, G. O., Irughe, M., Egharevba, E. & Akporhonor, B. A., (2022) Cloud Computing Application for accessing E-resources by University Librarians: Case Study of University Librarians in Niger Delta Region. *Library Philosophy and Practice (e-journal).* 7232 . https://digitalcommons.unl.edu/libphilprac/7232

Fernando, N., Loke, S.W. & Rahayu, W. (2013). Mobile Cloud Computing: A Survey. *Future Generation Computer Systems,* 29, 84-106.

Goyal, S. (2014). Public vs Private vs Hybrid vs Community-Cloud Computing: A Critical Review, *International Journal of Computer Network and Information Security*, 20–29. doi:10.5815/ijcnis.2014.03.03.

Irfan, M., Usman, M., Zhuang, Y. & Fong, S., (2015).A Critical Review of Security Threats in Cloud Computing', in 2015 *3rd International Symposium on Computational and Business Intelligence (ISCBI),* 105–111. doi:10.1109/ISCBI.2015.26

Meena, R., Sujeetha Devi, T., Vinodhini, R., Vishwam, R., & Yamini Priya, H. (2016). Design and Implementation of Virtual invigilation System and Smart Exam scheduler. *Advances in Natural and Applied Sciences,* 10(9), 367-374.,

National Institute of Standards and Technology, NSIT, (2012). National Institute of Standards and Technology 2–3

Rajaei, H., & Wappelhorst, J. (2011). Clouds & grids: a network and simulation perspective. 3rd April Spring Sim.

Raoa, R. V., and Selvamanib. K., (2015). Data Security Challenges and Its Solutions in Cloud Computing, in *Proceedings of International Conference on Intelligent Computing, Communication & Convergence (ICCC),* Bhubaneswar, Odisha, India, 204-209

Rohmeyer, P., and Ben-zvi, T., (2015) Managing Cloud Computing Risks in Financial Services Institutions, in 2015 Proceedings of PICMET '15: Management of the Technology Age, 519–526.

Rolim, C.O., Koch, F.L., Westphall, C.B., Werner, J., Fracalossi, A. & Salvador, G.S. (2010) A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. Second International Conference on e-Health, Telemedicine, and Social Medicine, St. Maarten, 10-15 February,2010,95-99.

https://doi.org/10.1109/eTELEMED.2010.19

Saranya, V., Ramya, S., Kumar, R. S., & Nalini, T. (2016). Efficient and Parallel Data Processing and Resource Allocation in the Cloud by using Nephele's Data Processing Framework. *International Journal of Grid and Distributed Computing*, 9(3), 33-40.

Sengar, S., (2015) SURVEY: Reputation and Trust Management in VANETs, *International Journal of Grid and Distributed Computing* 8(4), 301-306.

Soofi, A. A. and Khan, M. I. (2014) Encryption Techniques for Cloud Data Confidentiality, *International Journal of Grid and Distributed Computing* 7(4), 11–20.

Srivastava, S., & Sudhish, P. S. (2015, December). Security in cloud computing systems: A review of challenges and solutions for security in distributed computing environments. *In the 2015 39th National Systems Conference (NSC)* (1-5). IEEE.

Suzuki, H. and Juli, Y. (2017) 'Private Cloud Platform Based on Open Source Technology', FUJITSU Sci. Tech. J., 53(1), pp. 52–57

Xu, L. and Li, J., (2016) Building Efficient Resource Management Systems in the Cloud: Opportunities and Challenges, *International Journal of Grid and Distributed Computing*, 9(3), 157–172.