American Journal of Computer Science and Technology
2022; 5(3): 178-183
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20220503.14
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Hybridized Cryptography and Cloud Folder Model (CFM) for Secure Cloud-Based Storage

Anietie Ekong[1, *], Odikwa Henry[2], Abasiama Silas[1], Imou Douglas[1]

[1]Department of Computer Science, Akwa Ibom State University, Ikot Akpaden, Nigeria

[2]Department of Computer Science, Abia State University, Uturu, Nigeria

Email address:

anietieekong@aksu.edu.ng (Anietie Ekong), Ndubuisi.odikwa@abiastateuniversity.edu.ng (Odikwa Henry)

[*]Corresponding author

To cite this article:

Anietie Ekong, Odikwa Henry, Abasiama Silas, Imou Douglas. Hybridized Cryptography and Cloud Folder Model (CFM) for Secure Cloud-Based Storage. *American Journal of Computer Science and Technology*. Vol. 5, No. 3, 2022, pp. 178-183. doi: 10.11648/j.ajcst.20220503.14

Received: August 3, 2022; **Accepted**: August 27, 2022; **Published**: September 27, 2022

Abstract: Information security is the number one priority for any establishment concerned with its growth and privacy of its data. Attackers have devised a variety of strategies to get access to organizations' databases, both on cloud and offline systems. The incorporation of both cryptography and cloud folder model to secure cloud based storage presented in this paper, is a contemporary approach to securing cloud storage. The Cloud Folder Model adds to the storage strength. It serves as a significant deterrent against eavesdropping and injection assaults on the cloud storage. The model leverages RSA and AES data encryption, as well as a folder concept for storing the files in the cloud. It only enables authorized entities to have access to data and rejects suspicions and fraudulent attempts to access secured data. The system also created a mechanism that utilizes public and private keys. The system is be divided into two sections: online and offline. Data is encrypted using RSA and the Advanced Encryption Standard on the offline side (AES) while the online system adds to the encrypted data's security by guarding against injection attacks and data eavesdropping in transit. Our result shows that the new system provides better security for cloud storage than the existing system.

Keywords: Cryptography, Cloud Storage, Data Security, Cloud Folder

1. Introduction

Cloud computing has existed for some time. It is an innovative paradigm for delivering services and information utilizing current technologies, rather than a unique technology. Cloud computing, in its most basic form, makes use of existing internet infrastructure to facilitate communication between client nodes and remote services or applications [11]. Cloud service providers (CSPs) are responsible for providing cloud services that allow clients to create and use web services, similar to how internet service providers (ISPs) provide high-speed broadband for internet access. Cloud platforms, unlike the internet, serve as an abstraction layer between computer resources and the underlying low-level architecture. Cloud users do not need to own physical computing infrastructure; instead, they must pay a CSP subscription fee to access cloud infrastructure and resources [5].

The subscription model for cloud computing allows users to save money that would otherwise be spent on often-expensive resources such as hardware, software, and the associated licenses. Such services are provided by CSPs. The widespread use of cloud services has created a number of issues for users and CSPs. The most major difficulty, according to several researches, is creating and maintaining the security of services and information stored on cloud infrastructures. Muhammad P. et al. [6] noted that cloud computing concerns, notably data security and privacy protection, are the key barriers to future adoption of cloud storage. The report points out that the security problems in this sector of cloud computing stem from the fact that data and infrastructure management on cloud platforms is frequently handled by third parties that are unknown to clients [15]. Despite CSPs' efforts to provide extremely secure password-protected accounts, any signs of security lapse may result in the loss of clients and hence the cloud services business.

Nidhi, K. et al. [9] stated data security is the primary concern with cloud storage, according to the experts, who relate the difficulty to the fact that cloud storage includes several users sharing the same storage resources. Weak data access control and identity management procedures may jeopardize the security of data and information stored on cloud services. Due to the aforementioned issues, several technological techniques to improve the security of data and information kept on cloud platforms have been implemented. While there are numerous security solutions for cloud storage, we suggest a hybrid encryption strategy based on cloud folder to address SQL injection and eavesdropper interception of data in transit.

To secure the data, our suggested system will leverage RSA and AES data encryption, as well as a folder concept that will operate as a database, storing the files in the cloud. The folder model has the same storage approach as folders. It features a feature that makes the data it stores highly resistant to injection assaults. In general, the system will be divided into two sections: online and offline. Data will be encrypted using RSA and the Advanced Encryption Standard on the offline side (AES). While the online system adds to the encrypted data's security by guarding against injection attacks and data eavesdropping in transit.

2. Literature Review

2.1. Cloud Computing

Cloud computing is a new technology that allows cloud users to share and pay for resources on an as-needed basis. It's also a step forward in information technology and a popular business model for delivering IT services [17].

2.2. Overview of Cloud Storage Security

Cloud computing is a new technology that allows cloud users to share and pay for resources on an as-needed basis. Software, a single program, a platform, and bandwidth are examples of resources that a user can access over the internet. Because the cloud service provider must handle several requests, the cloud must be very scalable. Any cloud user can use a PC, tablet, smartphone, or laptop to access data from the cloud over the internet. Because cloud computing is such an effective paradigm, security and privacy have become a big and pressing concern for both cloud users and cloud services suppliers [1]. One key reason is that cloud customers rely on the cloud provider, and it is the cloud provider's responsibility to send data in a secure manner [1].

Cryptography is one of the widely established methodologies being used to secure the authentication, confidentiality, data integrity and access control of networks in industry and academics, and it is used to provide security. Many cryptography-based strategies have been utilized independently for cloud data security in recent years, with some studies focusing on secure storage, reliable computation, and secure service usage. A sub-offer within the cloud computing platform is known as the cloud storage facility [7]. Using this cloud storage, the customer is given their own space rather than having their data saved on dedicated cloud providers [13]. Data storage services are provided by the providers to Internet users and others. The primary demand of today's cloud storage providers is the ability to store a vast volume of data while maintaining a high level of security. Cyber-attacks (and data breaches) and regulatory compliance are the top issues when it comes to cloud computing security. The major problems, broken down further, center on visibility, access controls, and misconfigurations.

2.3. Cloud Features

Cloud computing has a few distinguishing characteristics that show how it differs from traditional computing processes. The US National Institute of Standards and Technology USNIST has specified the first five fundamental qualities listed below [2]. The following are some of the characteristics of cloud computing:

(a) on-demand self-service, where cloud users have total control over the computer resources [2].
(b) Broad Network, cloud users can use interfaces on heterogeneous thin and thick client platforms [2].
(c) Resource pooling or Provisioning, where multi-tenant models are used by cloud service providers to serve numerous customers.
(d) Rapid Elasticity and Scalability: The available resources' scalability appears to be limitless at any time for greater services. Nodes in the network can be added or removed with minimal infrastructure changes. It is automatically obtained and released in response to customer demand [2].
(e) Measured Service or utility-based Pricing: In this form of cloud, it enables transparency for both cloud providers and customers to maximize resource utilization.
(f) Location Independence: the cloud consumer has no idea where the hired resources from service providers are physically located. Many service providers establish data centers in various locations throughout the world in order to give optimum service utility and high network performance.
(g) Cost Effectiveness: The cloud can be set up near a cheap power plant and on low-cost real estate [2].
(h) Multi-tenancy: As a Shared Infrastructure characteristic, the cloud service provider can rent out a single infrastructure as a service to multiple customers by providing appropriate technical partitions called multi-tenancy and location independence, and has defined that cloud customers use physical services as virtualized software models based on their demand [2].

2.4. Overview of Cloud Services

Cloud service models are classified by the USNIST into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Each

service model has its own set of capabilities that serve as an organizational scope and demonstrate a level of abstraction over the computational environment [2]. Furthermore, according to a 2008 study by [21], cloud computing architecture is divided into five layers: Cloud Applications (SaaS), Cloud Software Environment (PaaS), Cloud Software Infrastructure (Computational Resources as Iaas), Storage as (DaaS), Communications as (CaaS), Software Kernel, and Hardware or Firmware (HaaS). Each layer relates to a level of abstraction that hides the underlying complex components and allows cloud clients to access resources more easily. Youseff L. [21] were among the first to try to create a common cloud computing ontology. The following are the many cloud service models: software as a service, platform as a service, infrastructure as a service and communication as a service.

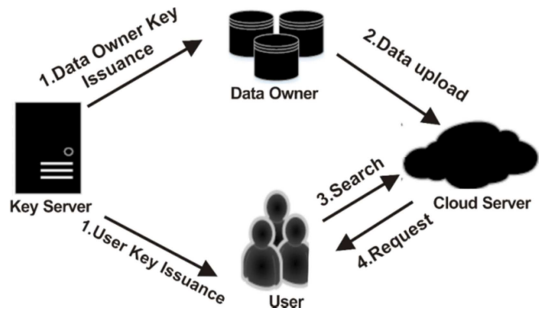

Figure 1. *General Structure of Uploading Data in Cloud Server [10].*

Supern, S. [18] discusses solutions being offered by cloud service providers like models, software as a service, platform as a service and infrastructure as a service. Sofia, M. et al. [14] developed a cloud based bio-informative analytic infrastructure and data management core for the expanded program on immunization consortium that used cloud-based architecture to track, save, store and share data that has biological samples during collection, shipping and processing while capturing meta data and associated clinical data.

Vasileios and Kostas [19] employed virus signature where antivirus programs use unique byte sequences for each virus so as to identify potential presence of malicious code in each file investigation procedure. It uses a hybrid security model for optimized protection and better virus detection which merges the sandboxing method system, system-changes-based signatures and cloud computing.

Vincent C. [20] employed the combination of multiple cryptographic algorithm of symmetric keys and steganography using triple data encryption standard, rivest cipher and advanced encryption standard algorithm to provide security to data. [9] employed blowfish and RSA/SRNN algorithm to secure data on the cloud. Sumagna, P. et al. [16] used a symmetric key cryptography algorithm and steganography using block-wise data security which is provided by AES, blowfish, RC6, and BRA algorithms to secure file in the cloud. Aman, S. et al. [3] focused on the file security and cloud storage security issues, giving particular attention to emerging trends and mechanisms of hybrid cryptography techniques.

3. Research Methodology

The system uses hybridized cryptography and cloud folder model (cfm). The process involves;

a) Designing the system using UML.
b) Building the system using RSA algorithm.
c) Uploading the encrypted cipher text to the cloud storage which is CFM.

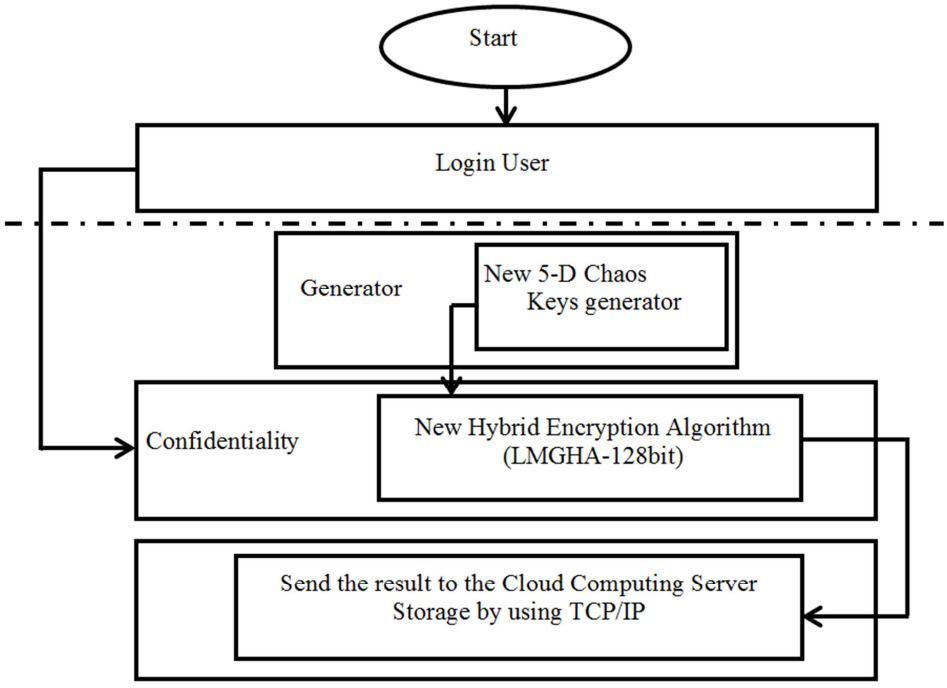

Figure 2. *The existing system architecture [8].*

Figure 2 shows the existing system architecture, which formed the bases for the extension of the new system shown in figure 3. Although the current method had several advantages, it also had major flaws that created a significant bottleneck in terms of information storage and security on cloud platforms. The system generated its security keys using a random number generator. These keys were short in length, with only a few characters combined and employed. It only takes a few well-planned tactics, such as brute-force, to break this type of security mechanism. We use RSA, an asymmetric key technique for encryption.

Not only were these the system's only flaws, but it also employed SQL statements to change its database, making the entire file in cloud storage exposed to unauthorized users and eavesdroppers. We make use of the Cloud Folder System because of the weaknesses in relational databases as it protects against attacks involving SQL statements and database manipulations.

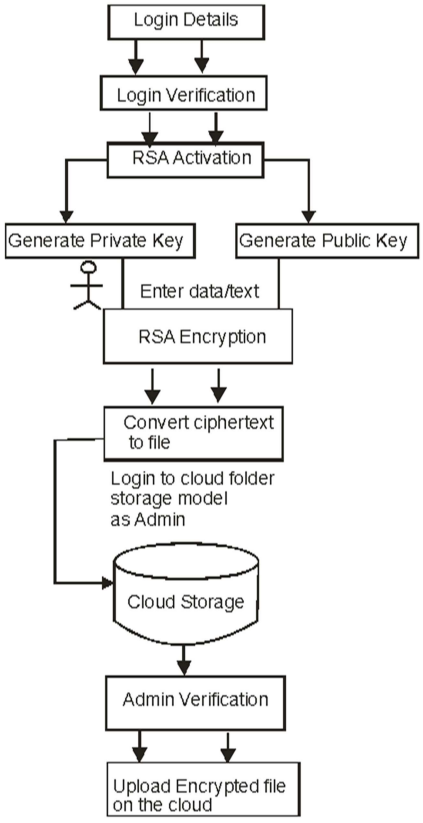

Figure 3. *Architecture of the proposed Hybrid System.*

The figure 3 shows the architecture of the hybrid CFM for secured cloud. It involves the login details and the verification of the login using the RSA activation. The RSA generates both the public and private keys, which when data is entered it uses the RSA encryption to convert the cipher text to file. This encryption ensures that within the channels that any intruder will not be able to decode the text. The converted text is stored in the cloud storage for the admin to verify and upload the encrypted file to the cloud.

Steps involved;

1) Login your details.
2) Call the RSA algorithm to generate public/private keys.
3) Feed-in the plaintext to RSA algorithm.
4) Encrypt the plaintext with RSA using public key.
5) Convert ciphertext to file (for CFM).
   Pseudo Code for ciphertext:
   a) Input: String plaintext
   b) Input: An integer between 0 and 25 representing the right shift of the character or an integer between -25 and -1 representing the left shift of the characters.
   c) Traverse each character in the plaintext one at a time.
   d) Transform the given character depending on encryption or decryption.
   e) Print the ciphertext.
6) Invoke Cloud login system to publish the file.
7) Encrypted file is being uploaded to Cloud.

Our proposed architecture keeps encrypted files in a model with an extra degree of security. We encrypt text and convert it to a file, which is then stored in the cloud. No SQL injection attack or brute-force approach can access or intercept the file on this system. Statistical and cryptanalysis attacks are also resistant to the system. As a result, we can demonstrate that the architecture of the suggested system above follows the objectives we specified previously in this paper.

3.1. The RSA Algorithm

The RSA algorithm each user has a pair of keys: one published publicly (known as the public key) and another stored in a secure location (known as the private key) [4, 12] created the RSA algorithm in 1978.

3.2. RSA Algorithm

The RSA algorithm holds the following features –

a) The RSA algorithm is a popular finite field exponentiation over integers, including prime values.
b) This approach uses sufficiently large integers, making it challenging to solve.
c) In this algorithm, there are two types of keys: private and public.

To work on the RSA algorithm, you must complete the following steps:

Step 1: Create the RSA modulus.

The first step is to choose two prime numbers, p and q, and then calculate their product N, as shown below –

$$N = p*q \tag{1}$$

Let N be the specified huge integer in this case.

Step 2: Deduce Value €

Consider the number e as a derived number larger than 1 but less than (p-1) and (q-1). The primary requirement is that there should be no common factor between (p-1) and (q-1) other than 1.

Step 3: Generate a public key

The given integers n and e are used to make the RSA public key public.

Step 4: Generate a Private Key

The numbers p, q, and e are used to generate Private Key d. The mathematical link between the numbers is shown below:

$$Ed = 1 \bmod (p-1)(q-1) \quad (2)$$

The Extended Euclidean Algorithm takes the input parameters p and q, and the formula above is the fundamental formula for it.

3.3. RSA Pseudocode

Begin

1. Choose two prime numbers p and q.
2. Compute

$$n=p^{*}q. \quad (3)$$

3. Calculate

$$phi = (p - 1) * (q-1). \quad (4)$$

4. Choose an integer e such that 1< e <phi(n) and gcd(e, phi(n))= 1; i.e., e and phi(n) are coprime.
5. Calculate d as d ≡ e-1 (mod phi(n)); here, d is the modular multiplicative inverse of e modulo phi(n).
6. For encryption, c = me mod n, where m = original message.
7. For decryption, m = cd mod n.

End

3.4. The Encryption Formula

Consider the following scenario: a sender sends a plain text message to a receiver whose public key is (n, e). To encrypt the plain text message in the current circumstance, use the syntax below.

$$C = M^{e} \bmod n$$

3.5. The Decryption Formula

The decryption procedure is simple and contains analytics for calculating in a methodical manner. The modulus of the result will be determined as follows:

$$Plaintext = C^{d} \bmod n$$

(if receiver C holds the private key d).

4. Results and Discussion

In order to test the veracity and validity of the hybridized system, the interfaces developed as shown in figures 4, 5 and 6 were used. The job requires assuring the safety of cloud-based files. Before uploading the file to the cloud storage folder, it is encrypted with the RSA algorithm and transformed to (.txt). This approach protects the file from any type of injection attack. The system's administrator (Adm) has full permissions to upload encrypted data to the cloud, as well as to download it to an offline storage location and decrypt it before it can be read in plain text.

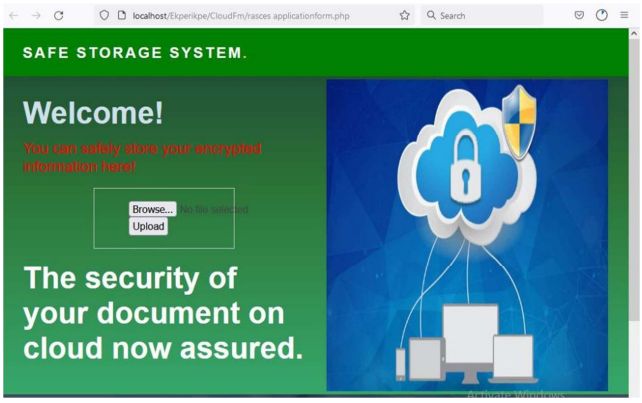

Figure 4. *Safe Storage Interface.*

Figure 4: depiction of the hybridized cryptography and cloud folder model interface.

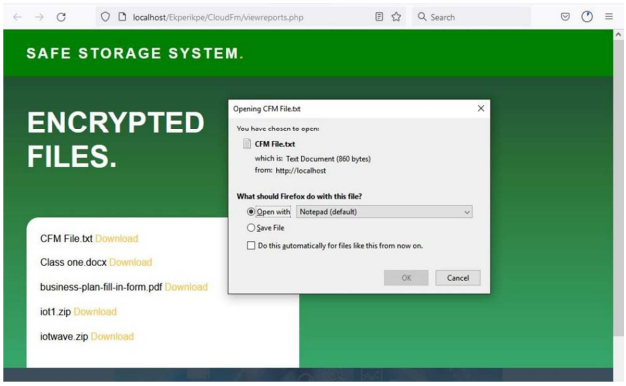

Figure 5. *Encrypted File Interface.*

The system keeps encrypted files in a model with an extra degree of security as shown in figure 5. The text is encrypted and converted to a file, which is then stored in the cloud. No SQL injection attack or brute-force approach can access or intercept the file on this system which were major drawback of most existing systems as in [8].

Figure 6. *Encrypted File Uploaded to Cloud.*

The job of uploading encrypted files requires assuring the safety of cloud-based files. Before uploading the file to the cloud storage folder, it is encrypted with the RSA algorithm and transformed to (.txt). This approach protects the file from any type of injection attack as shown in figure 6. The system's administrator (Adm) has full permissions to upload encrypted data to the cloud, as well as to download it to an offline storage location and decrypt it before it can be read in plain text.

In this system, we have two outputs: the encrypted cipher and the file converted to (.txt) file, which is transferred to the cloud system. Our plain text is encrypted and converted to cipher text via RSA. The cypher text is then saved as a text file (.txt). This file is then uploaded to the cloud which only the system administrator can download.

5. Conclusion

Over the years, studies have pointed to encryption techniques as effective instruments for ensuring information security. Since Relational Databases are vulnerable to SQL injection and other attacks, Cloud Folder Model proffers a better and more secure alternative for cloud storage. This research employed the RSA encryption method, which made use of two key ciphers: public and private keys. It assures that the security code used to protect information as saved in the cloud using CFM is safe. The system is operational and can be used to safeguard data from cyber eavesdropping, SQL injection hacking, and other miscellaneous cyber-attacks.

References

[1] Abubakar M., Aloysius A., Umar Z. & Dauda M., (2019). Comparative Analysis of Some Efficient Data Security Methods among Cryptographic Techniques for Cloud Data Security, Nigerian Journal of Basic and Applied Science, 27, (1), 81-88.

[2] Ahmad I., Bakht H. & Mohan U., (2017). Cloud Computing - A Comprehensive Definition. Journal of Computing and Management Studies. 1.

[3] Aman, S., Shivashankar, R., Ginni, and Advin, M. (2021). Securing File Storage on the Cloud using Cryptography. International Journal of Advanced Research in Computer and Communication Engineering. 10 (4), 265-268.

[4] Chang X., Li W., Yan A., Tsang P., & Poon T. (2022). Asymmetric cryptosystem based on optical scanning cryptography and elliptic curve algorithm. Scientific Reports. 7 (12). https://doi.org/10.1038/s41598-022-11861/

[5] Ghamya K., Suma K., & Bhargavi V., (2019). An Authorized ClouDedup in Hybrid Cloud using Triple Data Encryption Standard, International Journal of Recent Technology and Engineering (IJRTE), 8 (4), 9803-9807.

[6] Muhammad P., Sijjad A., Ghazala P. & Kamran A., (2019). SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms. International Journal of Computer Science and Network Security (IJCSNS), 19 (1).

[7] Muhammad R., Quazi M. & Rafiqul I., (2022). Lightweight cryptography in IoT networks: A survey, Future Generation Computer Systems, v129, p 77-89, ISSN 0167-739X, https://doi.org/10.1016/ j.future.2021.11.011

[8] Muhned H., Ghassan H. & Haider K., (2021). New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system, Turkish Journal of Computer and Mathematics Education, 12 (10), 2531-2540.

[9] Nidhi, K and Vimmi, M (2022). Secure Cloud Data storage using Hybrid Cryptography. International Journal for Research in Applied Science and Engineering Technology. 10 (4), 50-63.

[10] Pandey & Bathla, (2020). A Secure And Managed Cloud Storage System Using Encryption With Machine Learning Approach, International Journal of Science and Technology, 6, (3), 87-101.

[11] Priya (2018). Information Security And Privacy In Cloud Using Hybrid Cryptographic Algorithm, International Journal of Engineering Applied Sciences and Technology, 3, (4), 49-53.

[12] Rahul Neware, (2019). Survey on Security Issues in Mobile Cloud Computing and Preventive Measures, Smart Computing Paradigms: New Progresses and Challenges.

[13] Shynu P., Nadesh R., Varun G., Venu P., Mahdi A. & Mohammad R., (2020). A Secure Data Deduplication System For Integrated Cloud-Edge Networks, Journal of Cloud Computing: Advances, Systems and Applications, 9 (6), 100-109.

[14] Sofia, M. V Joann, D, Kerry, M, Shun, R… Ozonot, A.(2020). A Cloud based Bio-informatics Analytic infrastructure and Data Management Core for the Expanded Program on Immunization Consortium. DMC Journal. 6 (7), 104-110.

[15] Sood, S., (2021). A combined approach to ensure data security in cloud computing, Journal of Networking and Computer Application, 3 (5), 1831–1838.

[16] Sumagna, P., Sunil, A., and Rakesh, R. (2021). Hybrid cryptography algorithm for secure file Storage in the cloud. A Journal of Composition Theory. 9 (10), 25-28.

[17] Sunyaev A., (2020). Cloud Computing. In: Internet Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-34957-8_7.

[18] Supern, S (2011). Cloud Security in 21st Century: Current Key issues in Service Models on Cloud Computing. University of Nottingham.

[19] Vasileios, A. M and Kostas, E P (2014). A New Methodology based on Cloud Computing for Efficient Virus Detection. IEEE Conference.

[20] Vincent C., Michaela I., Wei B., Ang L., Qinghua L., Antonios, G., (2020). National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-210 Vttam, K and Jay, P.(2020). Secure File Storage on Cloud using Hybrid Cryptography Algorithm. International Journal of creative thoughts. 8 (7), 334-341.

[21] Youseff L., Butrico M., & Da Silva D., (2008). “Toward a Unified Ontology of Cloud Computing”, IEEE, 1–10.