International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

http://ijpsat.ijsht-journals.org
Vol. 27 No. 2 July 2021, pp.51-61

A Cloud Computing Platform On File Storage And Sharing Using Rijndeal Algorithms

Okafor, Loveth Ijeoma[1], Olayiwola Abisola Ayomide[2], Anozie Ekenechukwu Lilian[3], Idoko Nnamdi .A[4], Uzo, Blessing Chimezie[5], Royransom Nzeh[6], Ugwuanyi, Peace Nkiruka[7], Ikedilo, Obiora Emeka[8], Udenze, Loveth Ifunanya[9]

[1]Head It, Southeast Zonal Biotechnology Development Agency, University Of Nigeria, Nsukka
[2]Department Of Computer Science, Celeb University.
[3]Department Of Computer Science, University Of Nigeria, Nsukka
[4]Department Of Computer Science. Renaissance University, Ugbawka, Enugu.
[5]Department Of Computer Science, University Of Nigeria, Nsukka
[6]Department Of Computer Science, University Of Nigeria, Nsukka
[7]Centre For Distance And E-Learning, University Of Nigeria, Nsukka
[8]Department Of Computer Science, Akanu Ibaim Federal Polytechnic, Uwana.
[9]Department Of Medical Laboratory Science, Nnamdi Azikiwe University. Awka.

Abstract – In today's business world, every organization, companies and private individuals store their files online which is being monitored by untrusted individuals (Third Party) which are the manager and owner of cloud. Optimized security mechanism for file storage and sharing in a cloud computing platform using Rijndeal encryption algorithms is a platform to optimize the security of file and document against fraudsters. The goal of this paper is to implement file storage and sharing in a cloud computing platform using Rijndeal encryption algorithm. The proposed system aid encryption and sharing of encrypted files, it also lock the files in cloud before sharing it and ensure that users have full control of their files by using two factor authentications mechanism and encrypting the files before storing it which will prevent it from being hacked. Object-Oriented Analysis and Design methodology (OOAD) was used to analyze and design the system, whereas the implementation was carried out using PhP and My-SQL database management system. The accomplishment of this project enables firms, individuals and companies to store files and document in cloud environment without fear of any kind.

Keywords – ***File Storage, Cloud Computing Platform, Rijndeal Algorithms.***

I. INTRODUCTION

The Internet has become interwoven in our regular day to day existences and the quantity of individuals utilizing its administrations keep on developing quickly. As indicated by [1], there are currently more than three billion web clients overall which is 200% over the assessed clients that was recorded in 2005. Individuals utilize the web for various purposes, for example, cooperating through web-based media, conveying utilizing email, internet meeting instruments, shopping on the different web based business stages and online information stockpiling [2]. The cloud framework all in all is isolated into a few kinds as indicated by the clients and scope of cloud [3]. A similar cloud framework may serve various kinds of clients going from clients, endeavors and people. Rather than utilizing traditional arrangements, for example, neighborhood hard drives and glimmer drives, cloud information stockpiling permits clients to get to their information on the web. This methodology has numerous advantages, for

example, capacity to get to the data utilizing most gadgets, including workstations, tablets and advanced cells. It is additionally generally a basic undertaking to share information online with others or gathering by sending an association with empower them to get to a mutual organizer or transfer a solitary record. The reception of these distributed storage administrations was generous and this was supported in no little part by the quantity of suppliers competing to urge individuals to join to utilize their particular assistance. This contention among suppliers has brought about the measure of free space that people can get to. Likewise, rivalry among specialist co-ops has decreased the expense of information stockpiling charges. Nonetheless, information security has been viewed as one of the primary snags that are confronting the advancement of distributed storage administrations. As indicated by [4], a study of in excess of 500 Chief Technology Officer (CTO) and IT directors in 17 nations, demonstrated that regardless of the expected advantages of distributed storage, associations and people don't believe the current distributed storage specialist organizations due to the dread of the security dangers related with them. The security issues and danger related with distributed storage can be illuminate regarding data robbery, unapproved admittance to records or reports, phishing and social building assault and an appropriated disavowal of-administration (DDoS) assault. Huge numbers of such wrongdoing have been recorded. For instance, the examination on Internet extortion exercises on 23rd August, 2019 which included Obinwanne Okeke and others [5]. The examination by Federal Bureau of Investigation (FBI) evaluated that the tricksters swindled organizations over $10 Million which is the most noteworthy recorded web extortion up until now. They had the option to accomplish their questionable point by utilizing Business Email Compromise (BEC) tricks. The fraudsters utilized hacked email record of an association to persuade different organizations or people to make installment into their financial balance. Likewise, in [6], the creator clarified how cross-webpage scripting (XSS) which is PC security weakness found in web applications can be utilized to access records and reports. As per [6], XSS permit code infusion by vindictive web clients into the pages which will be seen by different clients. Instances of such code incorporate HTML code and customer side contents. A misused cross-site scripting weakness can be utilized by aggressors to sidestep access controls. These are because of the way that documents are put away in a public stockpiling suppliers' hard drive and nobody aside from the suppliers have authority over it and know where they are put away. A few scientists throughout the years have endeavored to proffer arrangement on network protection assault in cloud condition. For instance, an ongoing security weakness in the Dropbox encryption instrument [7] begins the discussions on whether distributed storage stages are sufficiently sheltered to store classified information. In [8], the specialist tried four distributed storage frameworks: Mozy, Carbonite, Dropbox, and Crash Plan. It was seen after the assessment that none of these frameworks can ensure information respectability, accessibility or even secretly.

II. THEORETICAL BACKGROUND

The theoretical background gives an outline of the technologies utilized in building up the framework "File Storage and Sharing Techniques in a Cloud Computing Platform Using Rijndeal Synchronous Key Encryption Algorithm" and the general idea of the research topic as observed by other researchers. The technologies are picked in order to introduce an easier way to use the framework. The project created comprises of different web contents written in HTML, CSS, JAVASCRIPT, PHP and MYSQL server which is utilized in the development of the database of the software.

2.1 ENCRYPTION ALGORITHMS

Encryption algorithm is a mathematical procedure for playing out an encryption on an information. During the time spent utilizing a calculation, data is changed over into good for nothing figure text which require the utilization of key to change the information once more into its unique structure. Today, quality of encryption is typically estimated by key size. Regardless of how solid the calculation, the scrambled information can be exposed to animal power assaults in which all potential blends of keys are attempted. In the long run the encryption can be split. For most current codes with nice key lengths, an opportunity to break them with savage power is estimated in centuries. Nonetheless, an undisclosed imperfection in a calculation or a development in PC innovation or numerical techniques could forcefully diminish these occasions. For the most part, the reasoning is that the key length ought to be appropriate for keeping the information secure for a sensible measure of time. In the event that the thing is extremely effective, for example, war zone interchanges or every day stock data, at that point a code that ensures it for merely weeks or months is okay. Nonetheless, something like your Visa number or public security privileged insights should be saved secure for a more drawn out period, successfully until the end of time. Thus, utilizing more vulnerable encryption calculations or shorter key lengths for certain things is alright, as long as the data helpfulness to an outcast lapses in a short measure of time. Some of Encryption calculations that can furnish great security highlights with rapid, less memory space during executions are

1. Rijndael Encryption Algorithm
2. AES (Advance Encryption Standard)
3. Blowfish Encryption Algorithm
4. RSA
5. 3DES.

Rijndael encryption algorithm was chosen for the development of this system and the reason will be stated in details later in this research work.

2.2 RIJNDAEL ENCRYPTION ALGORITHM

Rijndael is the algorithm, chosen by the U.S. Public Institute of Standards and Technology (NIST) as the possibility for the Advanced Encryption Standard (AES) [9]. It was chosen from a rundown of five finalists that were themselves chosen from a unique rundown of in excess of 15 entries. Rijndael will start to displace the Data Encryption Standard (DES) - and later Triple DES - throughout the following scarcely any years in numerous cryptography applications. The calculation was planned by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose last names are reflected in the code's name. The Rijndael algorithm is another age symmetric square code that supports key sizes of 128, 192 and 256 pieces, with information took care of in 128-piece blocks. Rijndael utilizes a variable number of rounds, contingent upon key/block sizes, as follows: 9 rounds if the key/block size is 128 pieces, 11 rounds if the key/block size is 192 pieces, and 13 rounds if the key/block size is 256 pieces. Rijndael is a replacement direct change figure. It utilizes triple attentive invertible uniform changes (layers). In particular, these are: Linear Mix Transform; Non-direct Transform and Key Addition Transform. Indeed, even before the first cycle, a straightforward key option layer is performed, which adds to security. From that point, there are Nr-1 adjusts and afterward the last round. The changes structure a State when begun yet before fruition of the whole cycle [9].

2.2.1 AES ALGORITHM

AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages. To provide security AES uses types of transformation. Substitution permutation, mixing and key adding each round of AES except the last uses the four transformations [10]

2.2.2 ATTRIBUTE BASED ENCRYPTION (ABE)

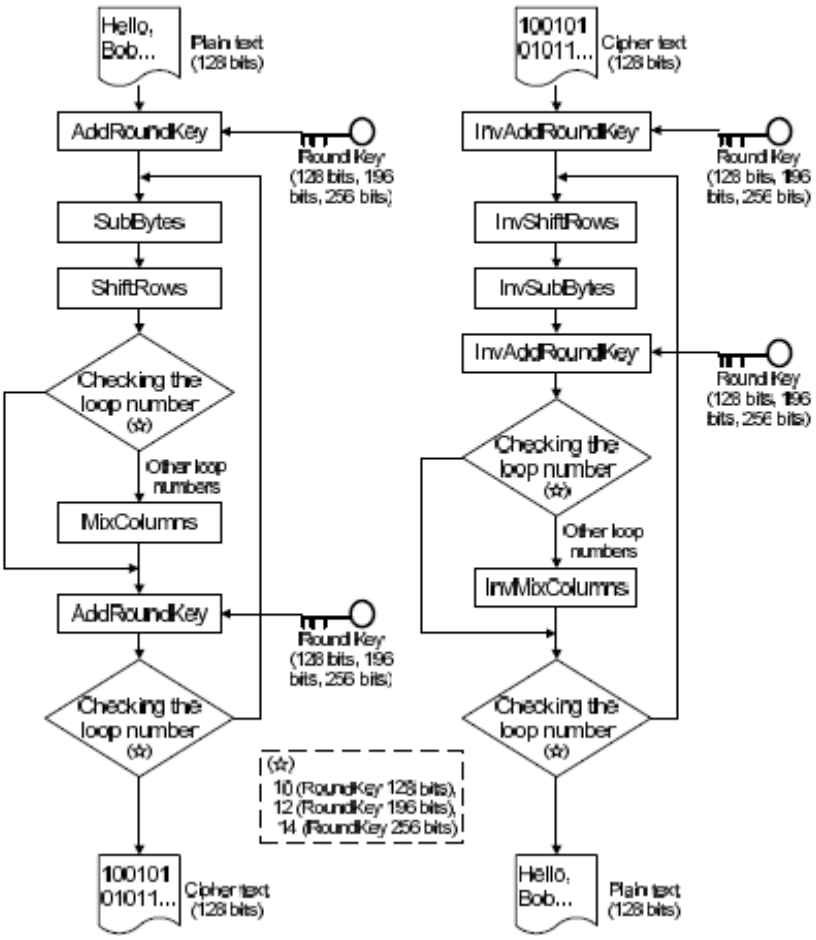
Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text [11]. A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. There are mainly two types of attribute-based encryption schemes: Key-policy attribute-based encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE) [12]. In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attributes. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attributes

2.3.3 BLOWFISH ENCRYPTION

This is a symmetric encryption algorithm invented by Bruce Schneier to replace popular Data Encryption Standard (DES). During the time of its development, almost all the encryption algorithms were protected by patents, government secrecy, or company intellectual property. Schneier in his kind gesture placed Blowfish in the public domain making it freely available for anyone to use. Blowfish is a 16-round Feistel cipher. It has block size of 64-bit and key sizes ranging from 32 to 448 bits.

2.3 IMPLEMENTATION OF RIJNDAEL ALGORITHM

The Rijndael algorithm is a notable cryptographic calculation that was reported as a swap for all the information encryption calculation by the National Institute of Standards and Technology (NIST) in 2000 and 2001. It is thusly a Federal Information Processing Standards (FIPS) affirmed cryptographic application [13]. The AES can change double private information into strong scrambled information. The AES calculation utilizes cryptographic keys called "Round keys" and 256 pieces to scramble and decode information in squares of 128 pieces. The AES is sorted as a square code calculation which ordinarily measures squares of 128 pieces from the first message by utilizing Round keys with an information length of 128, 192, or 256 pieces which makes it precarious. The encryption stream (Fig. 3(a)) utilizes four rudimentary changes called Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round Key, while the disentangling stream (Fig. 3(b)) utilizes the converse of these four rudimentary changes called InvSub Bytes, InvShift Rows, InvMix Columns, and InvAdd Round Key. The principle circles of the encoding/translating stream are rehashed 10, 12, or multiple times relying upon the Round key piece length (128, 196 or 256 pieces). For the essential handling of the AES calculation, squares of 128 pieces from the first message are masterminded into 4*4 clusters comprising of four sections and four lines containing 8-piece components called bytes.



(a) Encryption flow (b) Decryption flow

Fig 1. Processing flow Diagram of Rijndael Algorithm

2. 4 CLOUD COMPUTING

Cloud computing have diverse structure which make it to be seen in an unexpected way. Causing various understandings of them. Therefore, many consider cloud as online applications. Others consider it to be valuable or potentially equal registering in light of the fact that cloud is anticipated better and improved effectiveness in confounded and enormous scaled cycles [14]. Other than various states of cloud, the offered types of assistance are likewise exceptionally unique and various. Distributed computing have different definitions which some have been brought here. The definition by the public organization of standard and innovation of America is as per the following [15]: "Distributed computing is a model for empowering helpful, on-request network admittance to a mutual pool of configurable processing assets (e.g., networks, workers, stockpiling, applications, and administrations) that can be quickly provisioned and delivered with negligible administration exertion or specialist co-op collaboration." On other normal and adequate definition is of Ercan [16] "A profoundly versatile device, with the capacity of administration innovation empowered, which can be handily utilized by means of the web when required."

Following the meaning of distributed computing, we ought to grasp their significant highlights, created models, the method of utilizing administrations and furthermore the method of ensuring it, so as to know well and acknowledge it [17].

2.5 SECURITY IN CLOUD ENVIRONMENT

In the IT industry, the primary factor that will ensure the success of a system is information security [19]. Cloud computing is also a component of IT area, and in this rule, there is no exception and according to that the users of this technology don`t know where and how their information stored, the role of providing security becomes more important [20]. A number of security problems in cloud computing are provided with cloud models and others are provided by providing services models. So, security risks largely depend on service model and deploy of cloud [39] and this reduces the reliable services offers this technology. Offered Services by cloud computing because it provides services to the Internet, the protocols for normalization and security measures on the Internet are used to create the encryption and the security fixed part of needs somewhat, but they aren`t text-oriented and, therefore, a powerful set of policies and security contracts for the secure Transmission of data in the cloud is needed [21]. The subjects expressed below are refers to some of the risks of security-related data in cloud computing [22].

1) **Data position:** In the cloud environment, the issue of location of an organization or company data, (a place to host them, or even the country that data is located) is very challenging and controversial. One step to securing data is that to agree with provider cloud service to store and process your data in a specific geographical place. You can also use the legal obligations and require them to observe the integrity of your data.

2) **Data separation:** because in the cloud environment, many of data are stored in a shared environment. So, customers' data are together in a cloud. Provider cloud service must assure customers to make the data separated.

3) Flexibility of servers: Its full flexibility is one of the advantages of cloud computing and the fact that of this technology [23]. But this matter can cause some problems. Some servers may reconfigure back often without warning to the user. This matter can be challenging for the cloud inside`s data that related to a specific organization. So, if these changes continuously be applied the data security threatened.

2.5 REVIEW OF RELATED LITERATURE

This section, examines some of the previous approaches used by researchers for file storage and sharing techniques in a cloud computing platform. Below, we give a brief review of research studies that have been conducted using these techniques: RSA, DES, 3DES, RIJNDEAL.

According to [24], the security issues confronting distributed computing are information breaks, information robbery, and inaccessibility of cloud information. The scientist further recognized encryption as the main safety efforts that can be utilized to ensure records and information against the before referenced security danger.

In [25], proposed a Secure Storage and Access of Data in Cloud Computing that permit clients to safely store on the cloud and unreservedly access them when required. The proposed framework additionally guarantees that even the capacity supplier can't approach the information however just the appropriately confirmed client. The proposed framework utilized elliptic bend cryptography encryption strategy which has two sections specifically the private information area that stores the information which can be gotten to by the sender and a mutual information part that stores the information that will be shared between solid clients.

The issue with elliptic bend is that, it is hard to actualize the standard bends safely. In this way, elliptic bend isn't a best in class when contrasted with different norms like Rijndeal Algorithm.

According to [26], examined the distinctive between Data Encryption Standard (DES) and Rijndeal Algorithm with three fundamental highlights: (I) the capacity of the AES to oppose every distinguished assault, (ii) the straightforwardness and code scaling down on various stages and (iii) the effortlessness of the calculation plan. The scientists additionally took a gander at the benefits of AES over DES. The downsides of DES were additionally examined in their exploration. The significant preferences of AES over DES is its solid key which lessens the chance of having similar keys. Henceforth, the execution of Advanced Encryption Standards on various processor and equipment stage is conceivable.

In [27] proposed a Secured documents stockpiling on cloud utilizing mixture cryptography, a half breed of 3DES, RC6 and AES was concocted to execute information security in the cloud. These highlights, for example, Data uprightness, high security, low postponement and privacy were accomplished.

In [28], Proposed a Data Security of Mobile Cloud Computing on Cloud Server is an innovation for offering types of assistance, for example, programming, equipment and transfer speed over the Internet. Numerous organizations, for example, Apple, Facebook, Google and Amazon created versatile distributed computing. The scientist kept up that in as much as distributed storage administrations which has made clients of portable contraption to get to their information with especially simple and attractiveness that they ought to have security dangers at the top of the priority list. The analyst exhorted that the cloud worker supplier who deals with the information put away in cloud, can upgrade on the security of the information by apply encryption and decoding procedures before transferring information to cloud. Advance Encryption Standard (AES) was as encryption strategies for Mobile distributed computing (MCC) which would use as Encryption and Decryption methods. The disadvantage of the application is that it difficult to actualize it.

In [29], expressed the cloud offer registering stage that permit people and associations to execute various degrees of work, for example, online extra room and improvement of mechanized application programming. The specialist believed that as a result of the expansion number of the individuals utilizing the cloud each year, programmers are attempt to abuse the security weakness of the design of the cloud. Additionally, comparism of three cloud administrations models were examined. Seeing security issue; Cloud security dangers and dangers was dissected dependent on the kinds of the cloud administrations models; SaaS, Pass, IaaS. They likewise exhibition strategies that programmers control against cloud driving frameworks. The specialist was closed countermeasures against cloud security danger.

III. Description Of The Existing System

Data storage and recovery was worked on utilizing manual filling arrangement of organizing paper records that contains data on racks. These data stockpiles on racks are inclined to data robbery, data misfortune, and unapproved admittance to put away data. Over the long haul, the utilization of PC stockpiling framework was acquainted with store and offer data for people and association however it has its own container neck related with it which incorporates data being presented to different security danger since it isn't viably ensured. In this period of 21st century, there is an expansion in acknowledgment of Information Technology in taking care of different live issues. In this manner, distributed computing innovation was presented in the 21st century as an elective way to information stockpiling and data recovery with more extensive access and greater extra room. A case of existing stage for putting away and sparing information is Google drive. Google drive innovation was created by google in 1999 to handle the issue of capacity and to upgrade more accommodation to the clients [30]. The drive which was worked to store documents and films face genuine security challenges which incorporates giving unapproved admittance to data by the outsider who accessed email address. It likewise does not have an upgraded security engineering, and utilization of basic secret key to validate clients and access the board issue.

After a careful examination of the existing system, other problems that were identified:

(i) Lack of enhanced cloud security architecture and strategies

(ii) Use of simple password for user authentication in the cloud which is prone to hackers

(iii) Access management problems due to the cloud multi-tenancy exercise

(iv) Poor control of data access. It is virtually difficult to known who has access to the stored data

3.1 ANALYSIS OF THE PROPOSED SYSTEM

Having analyzed the features of the proposed system, it is quite obvious that the system will provide an enabling platform for its target users to safely store and share sensitive files on the cloud environment. The proposed system in order to solve the identified problems of the existing system, will employ the secured username and password authentication, One-time password (OTP) validation and File Encryption mechanism. We present a hybrid secure storage cloud architecture that allows an organization to store data securely in a public cloud and maintain information related to organization in private cloud. In this architecture, the user who wish to share or access data only interact with public cloud, there is no access for public users to access the private cloud. The public cloud is used to stored large amount of data. The encryption of data performed by data owner and decryption of data performed by cloud users. This architecture not only dispels the organization's concerns about risks of leaking sensitive structure information, but also takes full advantage of public cloud's power to securely store large volume of data. Another significant benefit of this architecture is that it overcomes collusion attacks such as the public cloud colluding with a revoked user, thereby allowing this user to decrypt data that has been encrypted to a role of which the user was a member previously.

3.2. SYSTEM ARCHITECTURE

The architectural design of the intranet-based wiki is of 3 (three) tiers as shown in figure 3.6. The tiers are the presentation, middle and data. The presentation tier is made up of the HTML, CSS and JavaScript. They are used for the frontend designs which include document structuring and styling. The middle tier comprises of the PHP code, which connects the presentation tier and the data tier. It is also in this middle tier that the firewall of the intranet, on which this wiki is based, is established for proper security of user data. The third, the data tier is for the database design, which serves as data repository which is needed by the system for processing of information. The database management system used for the design of this tier is MySQL. The middle and data tiers reside and function within the system server.

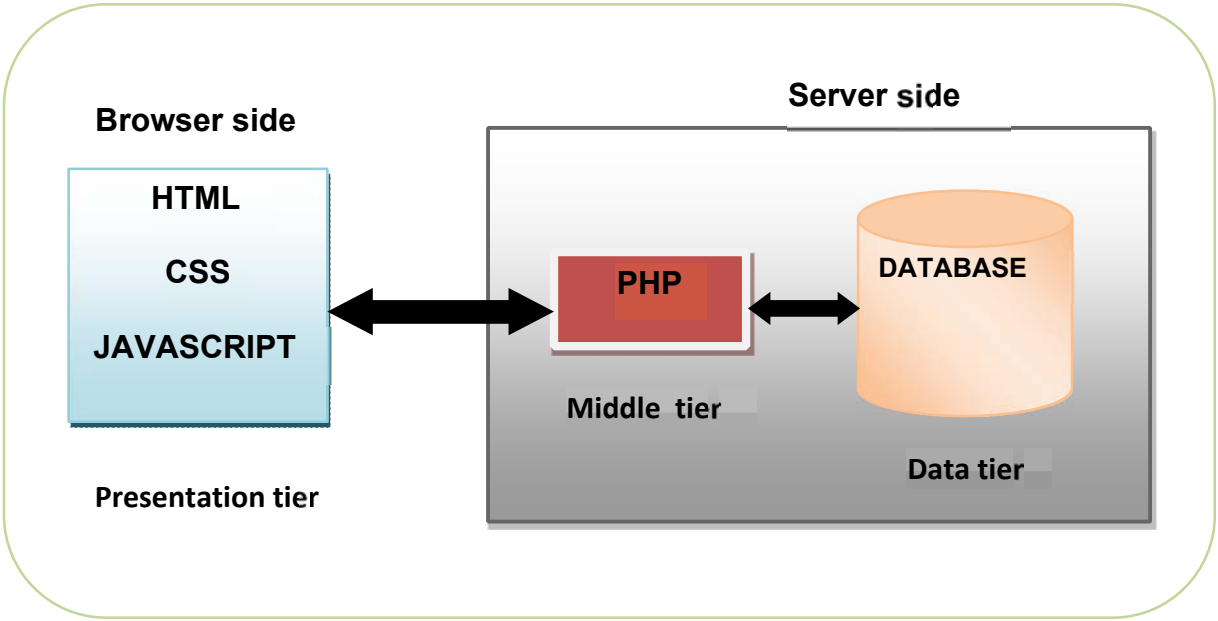


Figure 3: 3- tier web Architecture

IV. CHOICE OF DEVELOPMENT ENVIRONMENT

The integrated development environment (IDE) used in the development of this project is the Komodo editor 6.0, on which the source codes are written and tested on the Xamp server which is used as local host server on the Microsoft windows 7 platform. Chrome, Firefox or Torch are the browsers used. The Hypertext Markup Language (HTML) is the language or code used to edit and position the text, images, frames and other web page elements in this project. The development was made easy using PHP

programming language. PHP was chosen as the programming language to use because it is a widely used open source, general-purpose scripting language which offers the following advantage:

- It is fast
- It is free
- It is very easy to use
- It is versatile
- It is secure
- It is customizable

4.1 IMPLEMENTATION ARCHITECTURE

The implementation architecture of the Optimized Security Mechanism for File storage and sharing in a Cloud Computing Platform using Rijndael Synchronous Key Encryption is represented in figure 4.1 below. It is made up of the various components of the software modules and their linkages.

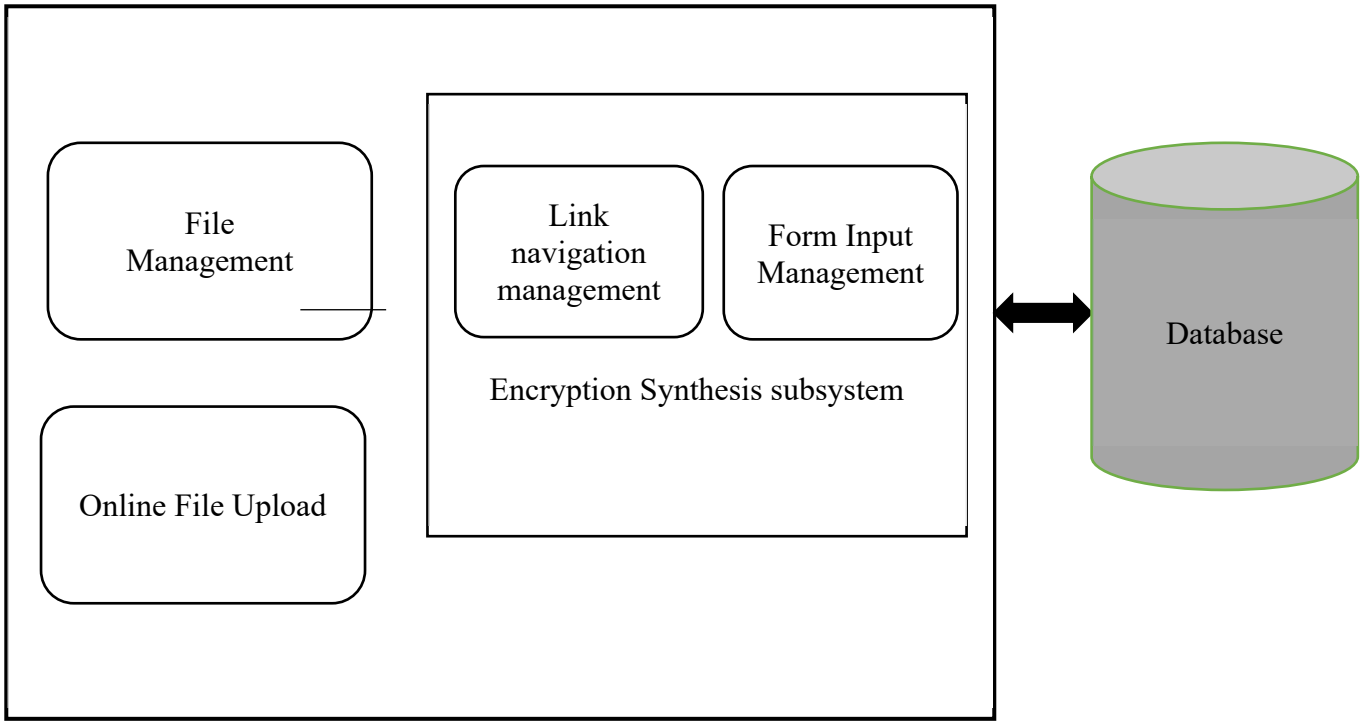


Figure 4.1: The Implementation Architecture

The Encryption Synthesis Subsystem is attached to all parts of the system, and it has two modules each of which handle the link navigation and form input. Most of the codes for Encryption are done with JavaScript. Figures 4.1 to 4.8 are the screen shots captured during the second phase testing of the system:

V. RESULT AND DISCUSSIONS

The main aim of this project is to develop "Optimized Security for File Storage and Sharing in a Cloud Computing Platform Using Rijndael Synchronous Key Encryption", an application that will help advance distributed computing security. The proposed framework is a cloud-based security framework that uses the Rijndael simultaneous key encryption instrument to make sure about

documents that are put away on the cloud by encoding the record way, lock the records and their indexes and furthermore award the client admittance to the cloud utilizing a two-factor confirmation system. The handiness of this undertaking is exceptionally clear because of the way that Internet use in business exchange and different works of life has expanded massively consequently making most web clients inclined to security assault, for example, data burglary, unapproved admittance to individual information and documents, phishing and social designing assault and a circulated forswearing of-administration (DDoS) assault. In this manner, it is fitting to shield clients of cloud administrations from the previously mentioned assaults utilizing the proposed framework. The proposed programming is an easy to understand online application that can without much of a stretch be gotten to once you are an authorized user.

5.1 CONCLUSION

The internet has become intertwined in our everyday lives and the number of people using its services continues to grow at a rapid rate. Hence, people use the internet for different purposes such as interacting via social media, communicating using email, online meeting tools, shopping on the various e-commerce platforms and online data storage. The proposed software is among the existing software solution for user that are facing security threat while using cloud services. The system was analyzed and designed with Object Oriented Analysis and Design Methodology (OOADM) and was developed using different web technologies such HTML, PHP and MySQL management system. MySQL management system was used as the database for storing data while HTML, PHP and other technologies such as JavaScript was used to develop the front end. Different literature relating to the topic of discourse was reviewed and this project improved on the identified gaps in literature.

The web has become interwoven in our regular daily existences and the quantity of individuals utilizing its administrations keeps on developing at a fast rate. Henceforth, individuals utilize the web for various purposes, for example, connecting through web-based media, conveying utilizing email, web-based gathering devices, shopping on the different internet business stages and online information stockpiling. The proposed programming is among the current programming answer for client that are confronting security danger while utilizing cloud administrations. The framework was examined and planned with Object Oriented Analysis and Design Methodology (OOADM) and was created utilizing diverse web innovations such HTML, PHP and MySQL the board framework. MySQL the executive's framework was utilized as the information base for putting away information while HTML, PHP and different innovations, for example, JavaScript was utilized to build up the front end. Distinctive writing identifying with the subject of talk was surveyed and this venture enhanced the recognized holes in writing.

REFERENCES

[1] B. Wellman "Physical place and cyberplace: The rise of personalized networking," *International journal of urban and regional research*, 2012, PP. 227-52.[PDF]. Available https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2427.00309

[2] S. Marston, S. Bandyopadhyay, J. Zhang and A. Ghalsasi." Cloud computing—The business perspective. Decision support systems" 2011, PP.176-89.[PDF]. Availablehttps://www.sciencedirect.com/science/article/pii/S0167923610002393

[3] T. Hoang, L. Chonho , D. Niyato and P. Wang. "A survey of mobile cloud computing: architecture, applications, and approaches." *Wireless communications and mobile computing* .2013. PP. 1587-1611.Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2427.00309

[4] J. Q. Anderson &H. Rainie "The future of cloud computing "(pp. 1-26). Washington, DC: Pew Internet &American Life Project.2010. PP. 1-26.[PDF].Available: https://s3.amazonaws.com/academia.edu.documents/7135848/the-future-of-cloud-computing.pdf?response-content

[5] BBC News. (2019, Sept.)." Letter from Africa: Why Nigeria's internet scammers are 'role models"[Online]. Available: https://www.bbc.com/news/world-africa-49759392

[6] S. Gupta, & B. B. Gupta" Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art*" International Journal of System Assurance Engineering and Management*. 2017. PP. 512-530.[PDF].Available: https://link.springer.com/article/10.1007/s13198-015-0376-0

[7] B. Chetan, K. Bhargavan, A. Delignat-Lavaud, and S. Maffeis. "Keys to the cloud: formal analysis and concrete attacks on encrypted web storage." In *International Conference on Principles of Security and Trust*,. Springer, Berlin, Heidelberg, 2013. pp. 126-146.[PDF]. Availble: https://link.springer.com/chapter/10.1007/978-3-642-36830-1_7

[8] E. Bocchi, D. Idilio, and M. Marco "Personal cloud storage benchmarks and comparison." IEEE Transactions *on Cloud Computing* .2015. PP 751-764. Available: https://ieeexplore.ieee.org/abstract/document/7096995/

[9] S. K., Rao, D. Mahto, & D. Khan."A survey on advanced encryption standard." *International Journal of Science and Research*, 2017,pp. 711-724.

[10] S. Singla, & J. Singh. "Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm" *Global Journal of Computer Science and Technology*.2013.Retrieved: https://computerresearch.org/index.php/computer/article/view/348

[11] G. Singh. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security". *International Journal of Computer Applications*.2013.PP.*67*(19).

Available: https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf.

[12] R. Saikeerthana, and A. Umamakeswari. "Secure data storage and data retrieval in cloud storage using cipher policy attribute based encryption." *Indian Journal of Science and Technology*. 2015.P. 318-325.

[13] J. Daemen, & V. Rijmen, (2002). *The design of Rijndael* (Vol. 2). New York: Springer-verlag. Available: https://link.springer.com/book/10.1007%2F978-3-662- 60769-5

[14] B.T Rao."A study on data storage security issues in cloud computing" *Procedia ComputerScience*.2018.P.128-135.Available: https://derby.openrepository.com/handle/10545/620916

[15] M.Hogan,F. Liu, A. Sokol, & J. Tong (2011). Nist cloud computing standards roadmap. *NIST Special Publication*, *35*, 6-11. Available: http://www.mofa-easj.dk/docs/cods/docs/NIST_Cloud_Computing_Reference_Architecture.pdf

[16] T. Ercan. (2010). Effective use of cloud computing in educational institutions. *Procedia-Social and Behavioral Sciences*, *2*(2), 938-942.

[17] D. Lin, & A. Squicciarini, (2010). Data protection models for service provisioning in the cloud. In *Proceedings of the 15th ACM symposium on Access control models and technologies* (pp. 183-192).

[18] I.A.T. Hashem, I. Yaqoob, N.B. Anuar, S. Mokhtar, A. Gani and S.U. Khan. "The rise of "big data" on cloud computing: Review and open research issues". *Information systems*.2015.*47*, PP.98-115.

[19] Y. Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science & Emerging Technologies, Vol-2 No 5 October, 2011.

[20] M. KapilSachdeva, "Cloud Computing: Security Risk Analysis and Recommendations", *Master Thesis, University of Texas, Austin,* 2011.

[21] F. Soleimanian, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", *International Journal Of Scientific & Technology Research*, Vol. 1, ISSUE 6, pp. 49-54, 2012.

[22] S. Pearson, "Privacy, Security and Trust in Cloud Computing", HP Laboratories, appeared as book chapter by Springer, UK, 2012.

[23] J. Hurwitz, R. Bloor, M. Kaufman, F. Halper," Cloud computing for dummies", *Wiley*, 2009.

[24] B. Trao."A study on data storage security issues in cloud computing" *Procedia Computer Science*.2018.P.128-135.Available: https://derby.openrepository.com/handle/10545/620916.

[25] S. Subashini & V. Kavitha. "A survey on security issues in service delivery models of cloud computing". *Journal of network and computer applications*. 2011. PP:1-11. Available:https://www.sciencedirect.com/science/article/pii/S1084804510001281.

[26] N. Penchalaiah and R. Seshadri. "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES)." *International journal of computer science and engineering* .2010.PP. 1641-1645.

[27] O.P. Akomolafe and M.O Abodunrin. 2017. "A hybrid cryptographic model for data storage in mobile cloud computing." *International Journal of Computer Network and Information Security*.2017.P.53.

[28] M. Waseem, A. Lakhan ."Data Security of Mobile Cloud Computing on Cloud Server.Open Access Library Journal". 2016 Apr.P30;3(1).

[29] I.A.T. Hashem, I. Yaqoob, N.B. Anuar, S. Mokhtar, A. Gani and S.U. Khan. "The rise of "big data" on cloud computing: Review and open research issues". *Information systems*.2015.*47*, PP.98-115.

[30] M. Aneke, and M. Wang" Energy storage technologies and real life applications–A state of the art review". *Applied Energy*, *179*, pp.350-377.2016.