IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.6, June 2021 E-ISSN: 2347-2693

Development of Security Model for Protecting Data in the Cloud Using 3-TIER Authentication

Agbakwuru A. Onyekachi[1*], Njoku D. Okechukwu[2], Amanze, B. Chibuike[3]

[1,3]Department of Computer Science, Faculty of Physical Sciences, Imo State University, Owerri, Nigeria.
[2]Department of Computer Science, School of Sciences, Imo State Polytechnic, Umuagwo, Owerri, Nigeria

DOI: https://doi.org/10.26438/ijcse/v9i6.3744 | Available online at: www.ijcseonline.org

Received: 17/Jun/2021, Accepted: 21/Jun/2021, Published: 30/Jun/2021

Abstract- This paper focuses on developing a security model for cloud computing to enhance the security for data stored in the database. Therefore this paper is providing a solution by designing a model for securing and protecting data in the cloud computing platform using National Identity Number (NIN), One Time Password (OTP) and Advanced Encryption Standard (AES). The design are simulated using a web-system developed with PHP, MySQL and JavaScript. The System Design followed the OOADM methodology for computerization of the system Modules giving room for coupling, decoupling, modification, encapsulation and reuse, as well as easy maintainability. Unified Modeling Language (UML) was extensively used to simplify the explanation of the system Modules. The software performance was tested using speed of data retrieval and security of the data protection. The security looks at the ability of the system to determine fraudulent users and deny them access to the system. The result obtained from the new system developed shows a high level of data security level as compare to existing system that uses only password for authentication.

***Keyword*:** OTP, AES, NIN, UML, NETWORK

I. INTRODUCTION

Data management and data protection is a burning issue across the globe. Agencies, ministries and individuals are looking for a more secured way of transmitting data. The global trend now is that technology is taking over every aspect of human lives more especially information dissemination. A lot of data manipulations are witnessed in transmitting records manually or semi-automated way. For example the Independent Electoral Commission (INEC) is having daunting challenges transmitting election results from pulling units to Local Government Area collection center and from there to State election collection center and finally to the collection center at Abuja. Most at times, at each center, the election results are altered to favor a particular candidate before it is transmitted to the next center. This portends a great danger to the nation. Also the electoral body is afraid of transmitting the election result electronically for fear of hackers manipulating the server and changing the results electronically. The last general election conducted in Nigeria shows that security of the electronic means of transmitting information is the sole reason why INEC denied or discarded results transmitted electronically and continued with the manual transmission of result. Looking at the trend of events in the developed countries, cloud computing tends to offer a more secured way of information dissemination electronically. Cloud computing includes a group of computers that are jointly used to provide different computations and tasks. Cloud computing is one of the most important IT paradigms in the last few years. One of the key benefits that is offered from this IT technology for the companies is reduced time and costs on the market. Cloud computing is providing companies and organizations to use shared storage and computing resources. It is better than to develop and operate with the own infrastructure. Cloud computing also provides organizations and companies to have a flexible, secure, and cost-effective IT infrastructure. It can be compared with the national electric grids that permit organizations and homes to plug into a centrally managed, efficient and cost-effective energy source. Main corporations including Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have invested in cloud computing and propose a range of cloud-based solutions to individuals and businesses. There are different types and models in cloud computing regarding the different provided services. The figure 1 describes the scenario where the total data of the local network resides within the Cloud, where the local network and the authorized users can access their data physically in the Cloud. At that instant of time, there exists a possibility for unauthorized users to enter and access the data in the Cloud. In this situation, the virtual machines are allotted to users of the Cloud. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways. Regarding this area of study, most of the research papers followed a normal traditional literature survey method. Few papers gave an innovative idea and proposed a security model. However, there are very few works, which considered the opinions of various security experts in Cloud Computing. This study proposes that, reader gets the true reflection of the security practices followed by various Cloud Computing companies in the current era. There are very few papers which focus on the security techniques for specified applications. Our work provides more knowledge in this dimension and also predicts the

future threats likely to be faced by Cloud Computing and solutions to these threats.

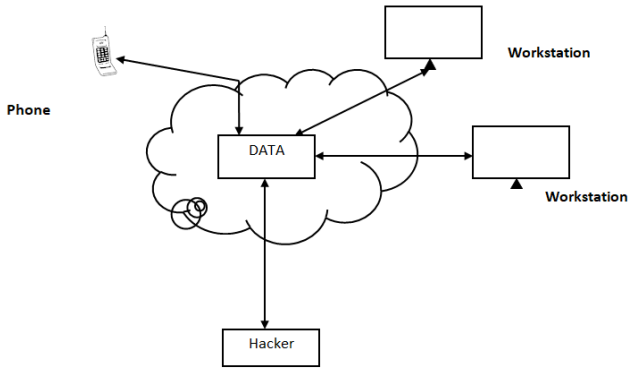

Figure 1. Unauthorized access of data within the cloud

Security and authenticity of information are the major fears that keeps most organizations away from cloud computing. People are scared of losing information to unauthorized persons. In the case of Independent Electoral Commission (INEC), safety and authenticity of election results transmitted online is the major factor that keeps the commission away from transmitting election result online. The documents transmitted could be intercepted and altered by hackers. The manual method of transmitting election results from pulling units to Local Government Area collection center and from there to State election collection center and finally to the collection center at Abuja is having big challenges. Most at times, at each center, the election results are altered to favor a particular person. Also, whenever the transmission is done online, it is protected using password and password is highly prone to attack. So there is need to look for a more reliable and secured way of protecting data in the cloud so as to enable INEC have the confidence of using the cloud computing technology for transmission of election results.

II. REVIEW OF THE RELATED WORKS

Cloud Computing

Cloud is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet (Kumar, 2016). Cloud computing as an emerging computing paradigm aims to share storage, computation and services transparently among massive users. Current Cloud computing systems poses serious limitation in protecting users' data confidentiality. Since users' sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the users' sensitive data by service providers may be quite high. There are many techniques for protecting users' data from outside attackers. An approach is presented to protecting the confidentiality of users' data from service providers, and ensures service providers cannot collect users' confidential data while the data is processed and stored in Cloud computing systems. Cloud computing systems provide various internet based data storage and services. Due to its many major benefits, including cost effectiveness and high scalability and flexibility, Cloud computing is gaining significant momentum recently as a new paradigm of distributed computing for various applications, especially for business applications along with the rapid growth of the Internet. With the rise of the era of "Cloud computing", concerns about "Internet Security" continue to increase. How will customers of the "Cloud" know that their information will be available to them, as well as secure and safe from others? The term "Cloud" in Cloud computing is the communication network or a network which is Combined with computing infrastructure. Cloud computing system is accessed using network which provides software, hardware, processing power etc. to the user when demand is generated. Cloud Computing is a virtual pool of computing resources which provides the pool to users through internet. Cloud Computing provides various services to user by creating group of clusters and grids of computers (Kumar, 2016). The main goal behind this is to provide services in virtualized manner to reduce burden of user to maintain everything by itself. It also refers to the web-based computing which provides devices with shared pool of resources, information or software on demand and pay per-use basis. Instead of having local servers or own devices to manage applications, people use sharing computing resources model of Cloud. The Cloud computing provides environment in which user can have its own virtual infrastructure using which they can perform tasks without depending on geographical boundary. Because of the flexible environment and cheaper cost, people are attracted towards the use of Cloud services that may be related to Platform, software or infrastructure. Based on the usage of Cloud, there are three deployment models: Public Cloud, Private Cloud and Hybrid Cloud. The Cloud computing provides a numerous advantages to its users but at the dark side it's also suffers from lots of issues like Integrity or Storage Correctness, Availability, Confidentiality and more. These issues make the adaption of cloud environment somewhat difficult for the users (Islam, 2015). Therefore lots of research is required in this direction to set a trust of Cloud user on Cloud service providers.

Security and Privacy Requirements in Cloud Computing

Protection of data is an important requirement while designing IT infrastructure of the organization. These requirements get even more stringent when data moves to cloud, and data becomes accessible through Internet. Therefore, strong authentication and access control mechanisms should be in place while deploying such systems.

Authenticity of Data: Data stored in cloud should be authentic, which means it should be possible to determine if the data is genuine and to verify the creator or owner of the

data (Rui, 2019). Deceptive data might result in unpredictable consequences, depending on use case scenario. Therefore, it should be possible to determine the owner of the data for further investigation. Note that owner or creator of the data may be a group or certain set of users. Authenticity of the data might be achieved by various signature schemes (Rui, 2019).

Authentication: Authentication of users and components is a crucial part of the collaboration in cloud. Data should be accessed only by the legitimate users. Therefore, all users are required to perform authentication process and getting authorized by the system, before allowing them to perform any other operations. Unauthorized access to the data might result in information leakages, data manipulation and other undesirable consequences.

Non-repudiation: Changing or deleting any valuable data might have significant consequences and result in money and reputation losses. Collaboration in cloud may deal with data provided by various data providers, and inconsistencies in these data might lead to reputation and money losses of data providers. Inconsistencies might occur by the ill-intentioned actions of the users and other involved parties. Non-repudiation property ensures that users cannot deny their transactions and actions on datasets (Iankoulova, 2018), and will carry responsibility over them.
Integrity: Collaboration in cloud may require large amount of data to be processed. Therefore, accuracy and consistency of processed data as well as obtained results should be preserved (Rui, 2019). Inconsistencies of the stored data might result in unpredictable consequences, depending on use case. For example, integrity violations may result in large amount of re-computations, and in wrong outcomes, which is unacceptable risk in some cases (e.g. healthcare systems).

Confidentiality: Unauthorized insiders or systems should not have permissions and ability to access data, which may considered as an internal documents, trade secrets, intellectual property, etc. In the cloud computing environment data is distributed over there mote servers that are shared with others and can be accessed through Internet or other connections. Moreover, collaboration might involve multiple cloud providers into business (Jonathan, 2020). These factors will increase the threat of data compromise in the cloud, since increased or even unknown number of access points will be available to the sensitive data (Piliouras, 2011). Therefore, serious confidentiality considerations should be taken into account, before moving data into the cloud. It is possible to achieve confidentiality through encryption mechanisms (Rui, 2019). However, in most of the cases data should still be search able in order to process queries on data sets and to support certain activities (Dan, 2015). Techniques like search able encryption or maintaining index of data might help in this case. Additionally confidentiality should be preserved while transporting the data (Piliouras, 2011), therefore encrypted channels like TLS, VPNs, etc. should be considered.

Availability: Users of a cloud should be able to access and use needed data resources on demand. High availability should be achieved, by preventing situations, such as Denial-of-Service attacks, power outages and hardware failures (Hamdi, 2017). Since cloud provides extensive processing power, organizations may perform their data analysis faster and effectively using cloud resources. However, analysis of data might suffer from unavailability of the data resources needed for analysis on demand.

Auditability: Audit procedures should be in place, in order to maintaining log of every access and modification of data in distributed environment (Iankoulova, 2018). Security breach notifications might be generated automatically based on logs. Audit logs might be stored and managed, however, it should be possible to reconstruct prior state of information and replay performed actions by combining relevant logs together. Audit logs might be the only way to track changes in the datasets. Additionally, confidentiality, integrity and availability of audit logs must be ensured.

Backup Procedures: All data stored in the cloud system should be backed up, in order to prevent data losses. Cloud service providers establish back up procedures to their customers as an indistinguishable part of their service. However, it might be risky to allow the cloud service providers to back up sensitive data and store it in distributed environment (Iankoulova, 2018). Even if built-in backup procedure is one of the benefits of cloud service, it might have a negative effect when sensitive data is considered.

Data Location Restrictions:
Data in the cloud is stored in the distributed manner, in the servers located all over the world. There is a need to restrict locations where cloud service provider will physically host the data (Arnon, 2020), before storing data or deploying corporative systems in the cloud. It is reasonable to avoid countries where intellectual property and privacy laws are inadequate and where data may be a subject of investigation due to the intrusive nature of the government.

Data Traceability and Labeling: All data stored in the cloud must be traceable in order to identify the origin of the leakage. Additionally, confidential data should be labeled, indicating that the data is proprietary and unauthorized usage of it will have legal consequences. These requirements are especially important in cloud environment, where increased vectors of information leakage present.

Data Segmentation:
Cloud computing benefits from resource sharing and virtualization mechanisms. That means multiple virtual machines are running on one physical machine and controlled by software hypervisor to keep appropriate separation of resources (Arnon, 2020). Cloud provides less separation than private IT infrastructures, where separate physical servers are deployed. So, there is a potential threat of data compromise through virtual machines running

under others control on the same physical server where sensitive data of certain organizations might be stored. Also, there is a risk of the network traffic capture in such cases. In ideal, data of separate parties should be processed and stored through unshared physical machines (Michaela, 2017), which is not the conception idea of a cloud computing. Therefore resource sharing must be limited to the minimum, depending on the agreement with the cloud provider. It is worth to note that, due to the resource sharing between different organizations in the cloud, forensic inspections of the storage will be a legal challenge. Aforementioned requirements should not be underestimated when moving to a cloud service, even if some of them are not feasible yet. Literally, control over the data is lost after the data has been moved to a cloud provider. It is not clear where data is resided and if data is disclosed to unauthorized parties. In a research, (Mohanaad, 2019) titled "Improving Authentication system for public cloud Computing", the researchers maintained that one of the most important goals of improving authentication system was to reach a high level of safety in the system and ensure the student's registration process clearly and also to work on the application of the One Time Password (OTP) algorithm which contributed to increase safety in the system by using the phone number in the account documentation. The results enable us to understand OTP algorithm structure and raise the level of protection for the system to protect it from hackers, one of the most important goals in this project is to reach a safety way that protects us from hacking and helps the student to obtain protection. Thus, having all the advantages can make the end-users satisfied and comforted with the used system. So, the system will be desired and wanted and also will be able to be reused and used in other organizations which means the success of the project. This research work centers on privacy and security of the cloud using OTP and didn't consider network availability which can lead to failure in delivering the OTP to the user's phone and this is the gap established in this work. Nayyarin his work (Nayyar, 2016), titled "Multi-Authority Authentication System for Cloud Data Storage", said that cloud data storage solutions constitutes a significant application area in the cloud computing domain. People and organizations are at will to, buy or lease the storage capacity for desired stipulated durations from these third-party service providers to store personal, organizational, or any application data. The subject proposition directly entails a secure authentication mechanism to ensure data confidentiality and integrity of vital digital data on the Cloud which may be available to multiple users, specifically in the case of multi-authority or group based digital systems. The researcher considers the Cloud as a platform to store group's data. The proposed protocol, at the macro level, comprises of three major stages, which incorporate group initialization, group member registration and group member authentication.

In order to validate our proposed protocol, they created different authentication mechanisms for each of the groups covering all possible combinations for creating and manipulating a group in a dynamic Cloud based environment. Group authentication, in its gamut offers certain vital problem areas which encompass effective access control, secure file access/transfer amongst group member(s), addition/revocation of group member(s) without repeated generation of new keys and preservation of group/data confidentiality in a dynamic cloud based scenario. Due to the aforementioned constraints, group authentication still remains a field not fully explored and thereby, presents a formidable research problem to develop a group authentication protocol in a dynamic cloud environment. In a research, (Agbasonu, 2017) titled "Cloud computing security for data at rest and data on transit", the researchers maintained that these measures such as encryption and password for data protection have loopholes and hackers know how to get their way through them. Encryption outputs (Cryptext) usually do have patterns with which to recognize the algorithm that produced it and quickly they design a reverse algorithm to decrypt and read the data. In the course of Passwords too, it was found out that passwords can be guessed, copied or hijacked. This research therefore provided a solution by designing an encryption model that can generate inconsistent cryptext with no pattern. Since illegal decryption is hinged on pattern matching, this encryption is therefore hack-proof. The research also designed a system of authentication that uses Biometrics instead of Password for access control. The advantages of having Biometric Systems in the cloud were given, such as reduction of cost and ubiquitous access. These designs are simulated using a web-system developed with PHP, MySQL, JavaScript and other Programs. The result obtained from the system shows that the system's encryption's cryptext is unique and cannot be decrypted with the conventional and contemporary illegal decryption systems. The system does not decrypt without additional input (Salt_key) from the user. This distinguishes the cryptosystem from others. The research gap in this work is that the key for salting the encryption is user dependent. A user having different keys for different data may forget or confuse the keys, since it is not stored in the database for security sake, there is need therefore to find out how to manage/retrieve these keys in case of user forgetfulness. Munjpara (Munjpara, 2018), proposed for Multi-tier Authentication Technique in cloud computing in his work titled "Implementation of Multi-tier Authentication Technique for Single-Sign On access of Cloud Services". The researcher was of the opinion that authentication is one of the major security parameters while providing access of the registered services to the intended users. Single-tier authentication relies on username and password for accessing the registered services which is not sufficient to secure from some well-known attacks like brute-force attack, replay attacks, etc. To provide a solution to this issue; he come up with multi-tier authentication using single- sign on access of registered services. Multi-tier authentication security relies on the username and password as well as pattern matching and one-time password (OTP). They proposed an authentication technique by modifying the existing two-tier authentication model to three-tier authentication with including the one extra authentication factor for verifying the intended user to overcome the insider attack and providing single-sign on

access of the registered services. The proposed authentication technique works on four phases. In the first phase, the users register themselves with the first-tier and second-tier authentication credentials. The first-tier authentication credentials are simple like username and password whereas the second-tier authentication credentials are like pattern matching or text field activity like in the existing technique. They took the pattern matching as the second-tier authentication credentials to simulating the proposed scheme. For the third-tier authentication, the user does not need to provide the authentication credentials like first-tier and second-tier authentication. They used mobile secret code as the third-tier authentication code. This secret code is valid for some amount of time to access the requested service. They provide the time limit with the secret code. After the time limit expires, the user cannot access the requested service with that secret code. The user needs another secret code for accessing the requested service. The result obtained shows that with increases as the number of authentication tiers in the system, the probability of success for breaking the multi-tier authentication system reaches near to the zero. Hence, by seeing the analysis of security, we can say that there is a very less probability of breaking the multi-tier authentication system. If we consider the usability of the storage space, then the proposed technique takes more space than the existing authentication technique which is very less and also we can say that it is negligible in the case of cloud environment where large amount of storage and its scalable. In 2019, Jan de Muijnck-Hughes proposed a security technique which is known as Predicate Based Encryption (PBE) in a research titled "Data Protection in the Cloud" (Muijnck-Hughes, 2019). PBE represents a family of asymmetric encryption and originates from Identity Based Encryption. This technique integrates Attribute Based Access Control (ABAC) with asymmetric encryption, thereby permitting a single encryptor/multi decryptor environment to be realized using a single scheme. This Predicate Based Encryption focuses its implementation at both Platform as a service and Software as a service. This proposed technique also precludes unwanted exposure, unwanted leakage and other unwanted breaches of confidentiality of cloud resident data.

III. MATERIALS AND METHODS

Different web application languages and modeling tools will be used to come up with a comprehensive protecting the data in the cloud. These include the following; Hypertext Markup Language (HTML), Hypertext Preprocessor (PHP), MySQL, Cascaded Style Sheet (CSS), Java Script, Dream weaver, Fireworks, SWiSHmax and Edraw. Dream weaver is an HTML-based application that is used to generate graphical user interfaces. The visual editing feature enables the creation of a web page without having to type HTML code. Dreamweaver supports graphics created by Fireworks or any other application so that one can easily import those graphics onto the web page. It also provides a coding environment with coding tools for users to edit HTML codes or to include any other scripting language. The scripting language behind the development of the credit card fraud detection is PHP. Other Scripting languages used are CSS and JavaScript. JavaScript is used to add functionality beyond standard HTML to a web page. It adds interactivity to web site. Edraw application was used to draw the UML diagrams. The choice of PHP and MySQL for this dissertation is because of the following benefits they offer. MySQL is commonly used together with PHP in website development and is popular open source software. A PHP and MySQL database driven site completely separates content and designing part. This way one only needs to update the database and the rest is taken care of by the system. Object-oriented analysis and design methodology (OOADM) was adopted in this research work and it is a set of standards for system analysis and application design. It uses a formal methodical approach to the analysis and design of information system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications. The main difference between object-oriented analysis and other forms of analysis is that by the object-oriented approach we organize requirements around objects, which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with. In other or traditional analysis methodologies, the two aspects: processes and data are considered separately. For example, data may be modeled by ER diagrams, and behaviors by flow charts or structure charts.

The primary tasks in object-oriented analysis (OOA) are:

- Find the objects
- Organize the objects
- Describe how the objects interact
- Define the behavior of the objects
- Define the internals of the objects

Common models used in OOA are use cases and object models. Use cases describe scenarios for standard domain functions that the system must accomplish. Object models describe the names, class relations (e.g. Circle is a subclass of Shape), operations, and properties of the main objects.

Sources of Data / Methods of Data Collection

In order to carry out a detailed analysis of the existing system, both primary and secondary data will be collected from different sources. Both secondary and primary data will be used to get facts on the subject where primary data will be collected from actual institutions and secondary data will be the data collected from literature review that include understanding and observing available cloud protection. Secondary data will also be gathered from a number of sources in order to carry out an insightful investigation into the existing systems, its working procedures, and its mode of operation. Secondary data include: internet sources, journals, books, newspapers and cloud computing.

Data Collection Tools
Due to the sensitive nature of the study, the methods used for primary data collection were limited to the person(s) involved who were reluctant to have any written document from them, the result where the following methods:

Person/Telephone Interviews: This is done by interviewing INEC employees from their personal experience on areas on the cloud computing that were prone to misuse by users or area already that had been misused by users. The key employees include branch managers, internal auditors and credit card officers.

Prototype System: This method proved to be very useful. Even though the INEC employees were reluctant to give information on the subject, when provided with a prototype system and asked to contribute on checks that could be put in the system to protecting data in the cloud.

IV. ANALYSIS OF THE SYSTEM

In cloud computing environment especially where client's application and data is stored in a cloud, users will interact with the cloud data sharing system through a Cloud-client application, which is also deployed in a cloud environment. Literally, Cloud-client application is a frontend service that performs most of the critical operations in the given architecture. Most of the data operations are performed only through Cloud-client application, such as data upload and data download. Operations, such as key generation, registration and retrieval are also performed only through the Cloud-client application. Cloud-client application is responsible for authenticating users before the start of any operations involving its intervention. Moreover, the Cloud-client application performs cryptographic operations while data upload and download. Cryptographic operations can be done more efficient in a cloud environment, with a flexible resource allocation and extensive computing power. Furthermore, Cloud-client application performs an authorization requests on behalf of the authenticated users and enforces the decisions made by a Policy Decision Point (PDP). Particularly, authorization requests to the PDP are done while data upload/download and key registration/retrieval.

This existing security model for protecting data in the cloud follows the following steps to complete the authentication process. Figure 2 illustrate below.

1. The user provides the URL of the cloud service provider in their web browser. The request is sent by the user's browser to the server of the cloud service provider. The cloud server loads the login GUI in the user's browser.
2. The user provides the username and password in the login GUI for passing through the first phase of authentication. These login credentials are passed to the server of the service provider.
3. The cloud server verifies the user for the username and password. If these credentials are correct, then the cloud server sends back the validation reply to the one application program that is observed on the client side.
4. If the system observes the correct password authentication entered by the user then the system initiate the original screen of the requested service.
5. After the initiating the original screen, the system loads the original screen in the user's web browser.
6. After loading the original screen in the browser, the cloud server makes the direct communication with the user for further activities in the loaded service.

Data Flow Diagram (DFD) of the Existing System

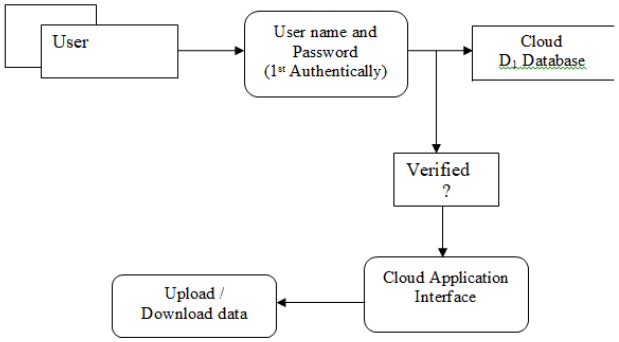

Figure 2: Data Flow Diagram of the existing system

Analysis of the New System
This paper used an authentication technique that made us of three-tier authentication with includes authentication factor for verifying the intended user to overcome the insider attack and providing single-sign on access of the registered services. The proposed authentication technique works on four phases. In the first phase, the users register themselves with the first-tier and second-tier authentication credentials. The first-tier authentication credentials are simple like username and password whereas the second-tier authentication credential is the National Identity Number (NIN). For the third-tier authentication, the user does not need to provide the authentication credentials like first-tier and second-tier authentication. The system is using the mobile secret code as the third-tier authentication code (One Time Password – OTP). This secret code is valid for some amount of time to access the requested service. We provide the time limit with the secret code. After the time limit expires, the user cannot access the requested service with that secret code. The user needs another secret code for accessing the requested service.

The paper scheme follows the following steps to authenticate the user for accessing the requested services. Figure 3 illustrated below.

1. For accessing the services, the user provides the URL of the cloud service provider in the web browser which sends the request to the cloud server for loading the Login GUI of the cloud service provider.
2. The user provides the registered username and password (first-tier authentication credentials) at the login GUI for verifying themselves to the cloud server.

3. If the username and password provided by the user to the cloud server is correct, then the cloud server sends the reply of validation at the user side. The application program or observer gets this validation reply at the user side.
4. The validation reply validates the user for the further authentication. If the cloud server sends the positive reply for validation, then the system request for the users NIN for further authentication.
5. Once the user supplies his/her NIN, the system links up the NIN database to authenticate the users identity
6. Once the user enters the NIN and submits this information to the application program, the system extracts his/her phone number from NIN database and sends the secret code (OTP) on the registered contact number of the user. This secret code has some time limit which is set by the cloud service provider. After the time limit, the code will be expired and no more use of that code.
7. The users provide the OTP which they got on their mobile number to the secret code submission screen for authenticating themselves.
8. Once the user provides the secret code to the system, it will match the code which it sends to the user and also checks the time limit of that code. If the user provides the correct secret code within the time limit, then the system initiates the code for loading the requested service in the web browser.
9. After initiating the code of requested service, the observer loads the requested service in the user's web browser.
10. Once the requested service is loaded into the web browser of the user, direct communication has been established between the user's web browser and the cloud server.

Once access is granted to the user, all data transmission will be encrypted using Advanced Encryption Standard (AES). AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data known as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. In this thesis, 128 bits AES algorithm was used and it uses a particular structure to encrypt data to provide the best security.

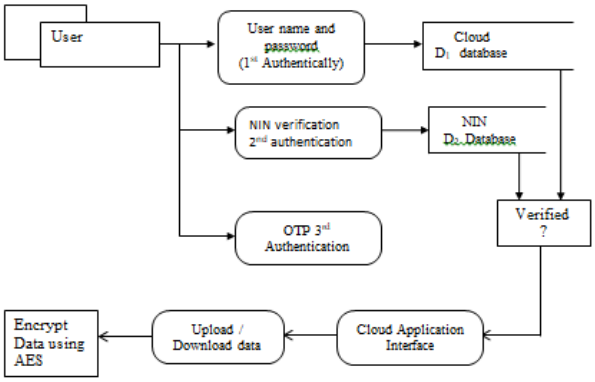

Figure 3: Data Flow Diagram of the proposed system

V. MATH SPECIFICATION

AES algorithm is based on AES key expansion to encrypt and decrypt data. It is another most important steps in AES structure. Each round has a new key. The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Where Nr is the number of rounds. The process is as follows:

The cipher key (initial key) is used to create the first four words. The size of key consists of 16 bytes (k0 to k15) that represents in an array. The first four bytes (k0 to k3) represents as w0, the next four bytes (k4 to k7) in first column represents as w1, and so on. We can use particular equation to calculate and find keys in each round easily as follows:

K [n]: w[i] = k [n-1]: w[i] XOR k[n]: w[i] 1.1

For w0 we have to use particular equation that is different from above equation.

K[n]: w0 = k [n-1]: w0 XOR SubByte (k [n-1]: w3>>8) XOR Rcon [i] 1.2

K_1:

W_0 = 0f 15 71 c9

W_1 = 47 d9 e8 59

W_2 = 0c b7 ad e8

W_3 = af 7f 67 98

How to find K2?

$K_2 = w_0 = k_1$: w_0 XOR SubByte (k1:w3>>8) XOR Rcon [2]

0f 15 71 c9 XOR SubByte (af 7f 67 98>>8) XOR Rcon [2]

Rcon [2] from Auxiliary function = 02 00 00 00

VI. CONCLUSION

Cloud based system faces a lot of security concerns and this scares organizations away from hosting their database in the cloud environment. Most security concerns centers on the privacy and validity of their data. This calls for more secured authentication system for cloud computing. Any authentication system's core strength depends upon the probability of success for breaking that system for accessing the services provided by the cloud service providers. In this thesis authentication scheme, the core

strength is first-tier, second-tier and third-tier authentication user credentials. For getting the access of the requested service, the attacker has to break all the authentication layers. At the first tier, the username and password of the user is verified. At the second tier, the NIN is verified by linking the NIN database and verifying the number provided. At the third tier, OTP is sent to the user's phone number and the user is expected to enter the OTP for final identification. Security analysis says that increases as the number of authentication tiers in the system, the probability of success for breaking the multi-tier authentication system reaches near to the zero. Hence, looking at the security model used in this thesis, one can say that there is a very less probability of breaking the multi-tier authentication system. Also the AES algorithm was used to secure the data more by encrypting the data stored in the cloud based database. With the above security measures, the data security in the cloud is guaranteed and it will encourage people to use cloud based systems as the security of data is guaranteed.

REFERENCES

[1] Arnon, R., Peter, M., Maya, H. L., Jean, S., David, K., & Patti, R. (2020). Methodological review: Cloud computing: A new business paradigm for biomedical information sharing. *J. of Biomedical Informatics*, 43(2):342–353, April 2020. 8, 9, 12

[2] Agbasonu, V.C. (2017). Cloud computing security for data at rest and data on transit. International Journal of Scientific Research and Innovative Technology ISSN: 2313-3759 Vol. 4 No. 2; February 2017.

[3] Dan, L. & Anna, S. (2015). Data protection models for service provisioning in the cloud. In Proceedings of the 15th ACM symposium on Access control models and technologies, SACMAT'10, pages183–192, *New York, NY, USA, 2015.ACM. 7, 12.*

[4] Hamdi, M. (2017). Security of cloud computing, storage, and networking. In Collaboration Technologies and Systems (CTS), 2017. *International Conference on, pages 1–5, May. 8*

[5] Islam, M.R. & Habiba, M. (2015). Agent based framework for providing security to data storage in cloud. In Computer and Information Technology (ICCIT), 2015 15th *International Conference on, pages 446–451, 2015. 13*

[6] Iankoulova, I. & Daneva, M. (2018). Cloud computing security requirements: A systematic review. In Research Challenges in Information Science (RCIS), 2018 *Sixth International Conference on, pages 1–7, May*

[7] Jonathan, S. (2020) .An application architecture to facilitate multi-site clinical trial collaboration in the cloud. In Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing, SECLOUD '11, pages 64–68, New York, NY, USA, 2020. ACM. 7.

[8] Kumar, A., Byung, G. L., HoonJae, L., and Kumari. A. (2016). Secure storage and access of data in cloud computing. In ICT Convergence (ICTC), 2016 *International Conference on, pages 336–339, 2016. 13.*

[9] Mohanaad, S. & Aaisha, K. (2019). Improving Authentication system for public cloud Computing.*Publication at: https://www.researchgate.net/publication/331035798*

[10] Munjpara, P. P. (2018). Implementation of Multi-tier Authentication Technique for Single-Sign On access of Cloud Services. Department of Computer Science and Engineering National *Institute of Technology, Rourkela Rourkela-769 008, Odisha, India*

[11] Muijnck-Hughes, J. (2019). Data Protection in the Cloud, 12 Jan, 2019 [Online], Available: http://www.ru.nl/ds

[12] Markus, J. & Faruque, A.S.M (2015). Mobile One Time Passwords and RC4 Encryption for Cloud Computing. School of Information Science, Computer and Electrical Engineering Halmstad University

[13] Niharika, G. & Rama, R.2015). Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography. *International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.2, April 2015*

[14] Nayyar, M. A. (2016) Multi-Authority Authentication System for Cloud Data Storage. Computer Science and Engineering Department Indian Institute of Technology, Kharagpur Kharagpur - 721302

[15] Piliouras, T., Pui, L.Y., Yang, S., Siddaramaiah, N., Sultana, E., Meyer, V.K.A. and Harrington, R. (2011). Trust in a cloud-based healthcare environment. In Emerging Technologies for a Smarter World (CEWIT), 2011. *8th International Conference Expo on, pages 1–6*

[16] Rui, Z. & Ling, L. (2019). Security models and requirements for healthcare application clouds.

[17] In Cloud Computing (CLOUD), 2019. *IEEE 3rd International Conference on, pages 268–275, July. 7*

