International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 11 - Issue 04 || April 2025 || PP. 52-61

An Enhanced Cloud Information Security System, Using Blowfish Encryption and Advance Encryption Standard (AES) Algorithms

Ugba Terkimbi Pius
Department of Computer Science and Statistics, Akperan Orshi Polytechnic, Yandev- Gboko, Benue State, Nigeria

Abstract: This research designs and develops a new security model for cloud computing to enhance Information Security using Blowfish Encryption and Advance Encryption Standard Algorithms. The proposed security model will improves the polytechnic performance by using minimum resources and management support, with a shared network, valuable resources as it provides a mechanism through which communication can be protected as well as hides the confidential information from unauthorized users. In this model, a combination of Advanced Encryption Standard (AES), Blowfish algorithm and Short Message Service (SMS) is implemented. Their combined features provides three way security i.e. confidentiality, authentication and verification. The proposed security system addressed issues of privacy, confidentiality, security and integrity of data stored in the cloud. This research will be of benefit to the polytechnic management, staff and the students of Computer Science Department. The resulting application is designed using Object Oriented Analysis and Design Method (OOADM) and is implemented using C# programming language and MYSQL data base.
Keywords: Information Security, Advance Encryption, Cloud, Application

Introduction

Cloud computing is a new model that can offer self-service on demand and at a negligible cost. It is gaining acceptance in all spheres including polytechnics, universities, government and non-governmental organizations. A study by Keiko H. *et al* (2013), considered Cloud Computing as the first among the top ten most important technologies and with a better prospect in successive years by companies and organizations. One of its benefits over in house IT infrastructure is the Total Cost of Ownership (TCO). Cloud services are easy to use and flexible to users; it has higher processing powers, on demand access and is cost saving and speedy. Despite the advantages of cloud computing there are some security challenges affecting in the adoption of the technology, one of the threats is data breaches. Data breaches is an incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an unauthorized individual. Also, Insecure Interfaces and APIs is another security threat to cloud application as general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempt to circumvent policy Manish, M.P *et al.,* (2013). Furthermore, abuse of cloud services is another challenge to cloud application as it has paved way for unauthorized users to illegally host software and other digital properties. Malicious users target users, organizations or other cloud providers through Distributed Denial of Service (DDOS) attacks, e-mail spam and phishing campaigns; mining for digital currency; large scale automated click fraud; brute force compute attacks of stolen credential database and hosting of fake cloud security alliance.

In addition, data loss may occur unless cloud consumer takes adequate measures to back up data. Other security challenges of cloud computing include application vulnerability, weak identity and weak password.

The cloud Services Interface must be designed to protect against both accidental and malicious attempt to circumvent policy. This could be through system vulnerabilities or insider threat to an organization may be the former employee or other business partners who had authorized access to it network. Therefore, Denial of access of Services (DOS) may prevent legitimate users to access their data.

As a panacea for security communication between the client and the server on the web and securing data stored in cloud, as earlier on proposed by others, through Secure Socket Layer (SSL) and Transport Layer Security (TLS). The researcher proposed a new security model for cloud computing. This model provides a mechanism through which information can be protected from unauthorized users. In this model a combination of AES and Blowfish algorithm will be implemented, there control features provide three way security i.e. confidentiality, authentication and verification as AES encryption algorithm is proposed for confidentiality of data, Blowfish algorithm for authentication and SMS for verification.

Statement of the Problem / Justification

Safeguarding the polytechnic data has consistently been a key issue in cloud computing because the data are stored in different machines and storage devices including PCs and servers. These confidential data

belonging to the polytechnic can be copied, modified or deleted by other users as a result of the open accessibility factor in cloud. It is the responsibility of cloud service providers to secure users' confidential data from unauthorized access. So, for providing an active and secured data security for the polytechnic, there is need to develop an effective security mechanism that provides data security in order to prevent data from disclosure and theft by unauthorized users. This research work, proposed a security framework that enables the polytechnic management to have adequate control over their data stored in the cloud.

Literature Review

Deepika V. and Karan M.(2014).Proposed a design that utilized the homomorphic token and distributed erasure-coded data to address the problem of security threat and improved security and reliable cloud storage service to realize a distributed storage integrity auditing mechanism. The design allows users to monitor the cloud storage with very lightweight communication and computation costs. This provides strong cloud storage accuracy, and also allows for faster fault location data, that is to say, the identification of misbehaving server. The proposed design supports continued safe and efficient dynamic activities, including block modification, deletion and append. The proposed system is very effective against server colluding attacks and data modification attacks .In their research Sumita, and Ajay(2014).proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. To ensure the security of data, they proposed the use of DES (Data Encryption Standards) algorithm. They provided a working architecture of Cloud data security using DES algorithm, which lets data stored in the database as cipher text and on request data is available in the required format. They rely on an erasure correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, their scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, they can almost guarantee the simultaneous identification of the misbehaving server(s). They used DES algorithm with erasure-correcting technique for providing data security with integrity.

A framework was developed by Deepika and Karan (2014) to enhance security while storing multimedia files which includes role base access control, encryption, and signature verification**.** The framework includes a premium and normal user concept in which a normal user would get a normal speed where as the premium user would get more speed. To encrypt large messages a hybrid approach was used in which the messages were actually encrypted using symmetric schemes (TDES) and the key was transported using asymmetric schemes (Diffie Hellman Key Exchange). The combination of encryption algorithms encrypts the data files before storage on cloud. In the proposed architecture, firstly Diffie Hellman algorithm was used to generate keys for key exchange step. Then TDES encryption algorithm was used to encrypt or decrypt user's data file.

Manoj K. and Kranti A. (2014). proposed a model to enhance security of cloud by using Station to Station key agreement for generating session key with a fixed timestamp between User and Cloud Server and then send request for any service by using Digital Signature Standard, the request message would be encrypted by using that session key which was shared earlier and once a session key is used then that session key would not be used again. So the user requires a new key for each session. All of these issues related to authentication and authorization are handled by a cloud manager present between cloud server and user.

Sumita, L. and AjayK. (2014).Proposed a web application in which users can store and transit data securely. This web application named "Impregnable Store", allows a user to access the data from anywhere at any time. Users can upload, download or view the data (either it is file, document, videos or photos) easily. The proposed web application is HTTPS enabled and provides a secure environment to store and safeguards all the data. The proposed cloud environment ensures authentication, data confidentiality, user oriented access control and availability. At the time of registration users enter some details like name, email address, password, secret code, date of birth etc. All the entered fields are checked for integrity and users must be 18 and above age and email address must be valid for future reference.

Sudhansu R. L. and Biswaranjan N. (2014). Proposed a new security model that provides a mechanism through which we can get secure communication as well as hides the information from unauthorized users. In this model they implemented a combination of RSA encryption and digital signature technique which can easily be utilized with all types of cloud computing features like: PaaS, SaaS and IaaS. This combination mechanism provides three way security i.e. data security, authentication and verification. In this paper, they proposed RSA encryption algorithm for confidentiality of data and MD 5 algorithm for authentication.

Ranjit K. and Raminder, P. S. (2015).Implemented a security model in Cloud Analyst to tighten the level of cloud storage security, which provides security based on different encryption algorithms with integrity verification scheme. They began with the storage section selection phase divided into three different sections Private, Public, and Hybrid. Various encryption techniques are implemented in all three sections based on the

security factors namely authentication, confidentiality, security, privacy, non-repudiation and integrity. Unique token generation mechanism implemented in Private section helps ensure the authenticity of the user, Hybrid section provides On Demand Two Tier security architecture and Public section provides faster computation of data encryption and decryption. Overall data is wrapped in two folds of encryption and integrity verification in all the three sections. The user wants to access data, required to enter the user login and password before granting permission to the encrypted data stored either in Private, Public, or Hybrid section, thereby making it difficult for the hacker to gain access of the authorized environment.

Nithya, C. *et al.,* (2016). Proposed a secure system for the storage of data in the cloud. To become eligible to store data a user has to register with the cloud database. This prevents unauthorized access. The files stored in the cloud are encrypted with RSA algorithm and digital fingerprint for the same has been generated through MD5 message digest before storage. The RSA provides unread ability of data to anyone without the private key. MD5 makes it impossible for any changes on data to go unnoticed. After the application of RSA and MD5 before storage, the data becomes resistant to access or modifications by any third party and to intruders of cloud storage system. This application is tested in Amazon Elastic Compute Cloud Web Services.

Cloud Delivery Models

The architecture of Cloud computing can be categorized according to the three types of delivery models Mohammed, A *et al.,* (2012).

i. **Infrastructure as a Service (IaaS):** Consumers are allocated computing resources in order to run virtual machines that consist of operating systems and applications that are provided as an on-demand service. The best example of IAAS is Amazon.com's Elastic Compute Cloud (EC2) service. The requirements of security beyond the basic infrastructure are carried out mainly by the cloud consumer.
ii. **Platform as a service (PaaS):** Cloud consumers are allowed to write applications that run on the service provider's environment. It is a model of service delivery where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Google Apps engine is an example of PAAS. The requirements of security are split between the cloud provider and the cloud consumer.
iii. **Software as a service (SaaS):** Cloud consumers are provided with various software applications that run over the internet. Google Docs programs are an example of SAAS. The requirements of security are carried out mainly by the cloud provider.

Cloud Deployment Models.

According to Satarupa B., and Abhishek M. (2013).Deployment models broadly characterize the management and disposition of computational resources for delivery of services to consumers, as well as the differentiation between classes of consumers. They listed the different deployment models as:

i. **Public Cloud:** A public cloud is one in which the infrastructure and computational resources that it comprises are made available to the general public over the Internet. It is owned and operated by a cloud provider delivering cloud services to consumers and, by definition, is external to the consumers' organizations.
ii. **Private Cloud:** A private cloud is one in which the computing environment is operated exclusively for a specific organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data centre or outside of it.
iii. **Community Cloud:** A community cloud falls between public and private clouds. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.
iv. **Hybrid Cloud:** Hybrid cloud is the most complex model among all the deployment models. They involve a composition of two or more clouds (private, community, or public). Each cloud remains a unique entity, but is bound to the others through consistent or proprietary technology that enables application and data portability among them.

Cloud Security Issues

According to Jens-Matthias B. et al. (2013).Security is a big challenge in cloud systems due to its nature of outsourced computing mainly, confidentiality, integrity and authentication are the primary pain areas. Unless robust security scheme and user-centric security policy is implemented, cloud system would be vulnerable to different attacks and susceptible by the users Arijit U., Debasish J., and Ajanta D. (2013).

According to Jens-Matthias B. *et al.,* (2013), the main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes.

When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the owner's control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. Depending on the political context this trust may touch legal obligations. For instance, Italian legislation requires that government data of Italian citizens, if collected by official agencies, have to remain within Italy Jens-Matthias B. *etal*., (2013). Thus, using a cloud provider from outside of Italy for realizing an e-government service provided to Italian citizens would immediately violate this obligation. Hence, the cloud users must trust the cloud provider hosting their data within the borders of the country and never copying them to an off-country location (not even for backup or in case of local failure) nor providing access to the data to entities from abroad.

An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously Jens-Matthias B. *et al*.,(2013). An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data. Even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider.

Methodology

The methodology used for designing this application is Object Oriented Analysis and Design Method (OOADM) and is implemented using C# programming language and MYSQL data base. The new security model provides a mechanism through which communication can be protected as well as information being hidden from unauthorized users. In this model, a combination of AES and Blowfish algorithms will be implemented. This combined features provides three way security i.e. confidentiality, authentication and verification. In this work, AES algorithm is used for data encryption and decryption purpose, Blowfish algorithm for authentication and SMS for verification.

The main technologies used for designing the new application are HTML, MySQL and C# programming language.

HTML is a hypertext mark-up language which is in reality a backbone of any website. This project is composed of web documents, that is, files written in HTML. The web documents are rendered to be visible (or presented) to the user by an application program known as a web browser. Each of the HTML documents is a sequence of elements. An element consists of start tag <title> content, and a closing tag in that order </title>.

SQL stands for Structured Query Language. SQL is used to create access and manipulate databases. MySQL Database Management System: MySQL queries will be used in the application to create, insert, update, retrieve and delete data from the underline database

Analysis of the Proposed Information Security System in Cloud Computing Using blowfish Encryption and Aes, Algorithms and Short Message Service (SMS)

The researcher proposes a new security model that provides a mechanism through which communication can be protected as well as confidential information being hidden from unauthorized users. In this model, a combination of AES, Blowfish algorithms and SMS will be implemented. This combined features provides three way security i.e. confidentiality, authentication and verification. In this work, AES algorithm is used for data encryption and decryption purpose, Blowfish algorithm for authentication and SMS for verification. The block diagram of the proposed security model is showed in the figure below

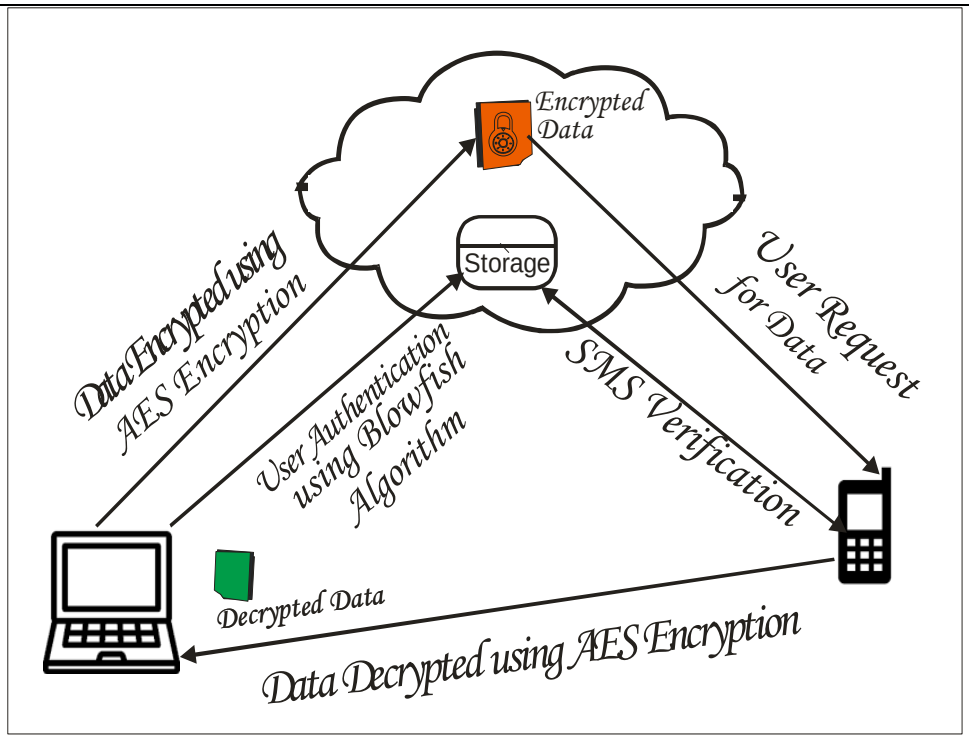

Figure 1: Proposed Security Model

To ensure a secure communication between the user and the cloud provider, the user data are encrypted while in transit to the cloud provider. AES encryption algorithm encrypts the user's data by using the systems public key. For successful transfer of data into the cloud for admission, the user will first be authenticated using Blowfish algorithm. Similarly, when the user requests for data, the system sends a verification code to the user's mobile phone for verification. After successful verification, the user's data are decrypted using the AES algorithm. Therefore AES encryption algorithm ensures secure communication between the user and the cloud provider.

Blowfish Algorithm

Blowfish is a symmetric encryption algorithm, meaning that it uses the same key to both encrypt and decrypt messages. According to Vaudena, S (1996). Blowfish is also a block cipher, meaning that it divides message up in to fixed length blocks during encryption and decryption. Pia, S. and Karamjeet, S (2013).Contained that, the Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64 bit block cipher and is suggested as a replacement for DES. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors, Pia, S. and Karamjeet, S (2013).

Basically, Blowfish encryption algorithm is requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles. According to Saikumar, M. and Vasanth, K. (2015). Blowfish contains 16 rounds. Each round consists of XOR operation and a function. Each round consists of key expansion and data encryption. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round feiestek network methods. Plain text and key are the inputs of this algorithm. Figure 3 shows how blowfish algorithm works. 64 bit plain text taken is divided into two 32 bits data and at each round the given key is expanded and stored in 18 p-array and gives 32 bit key as input and XORed with previous round data.

Then, for i = 1 to 14:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P15 and xL = xL XOR P16.

Finally, recombine xL and xR to get the cipher text. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.

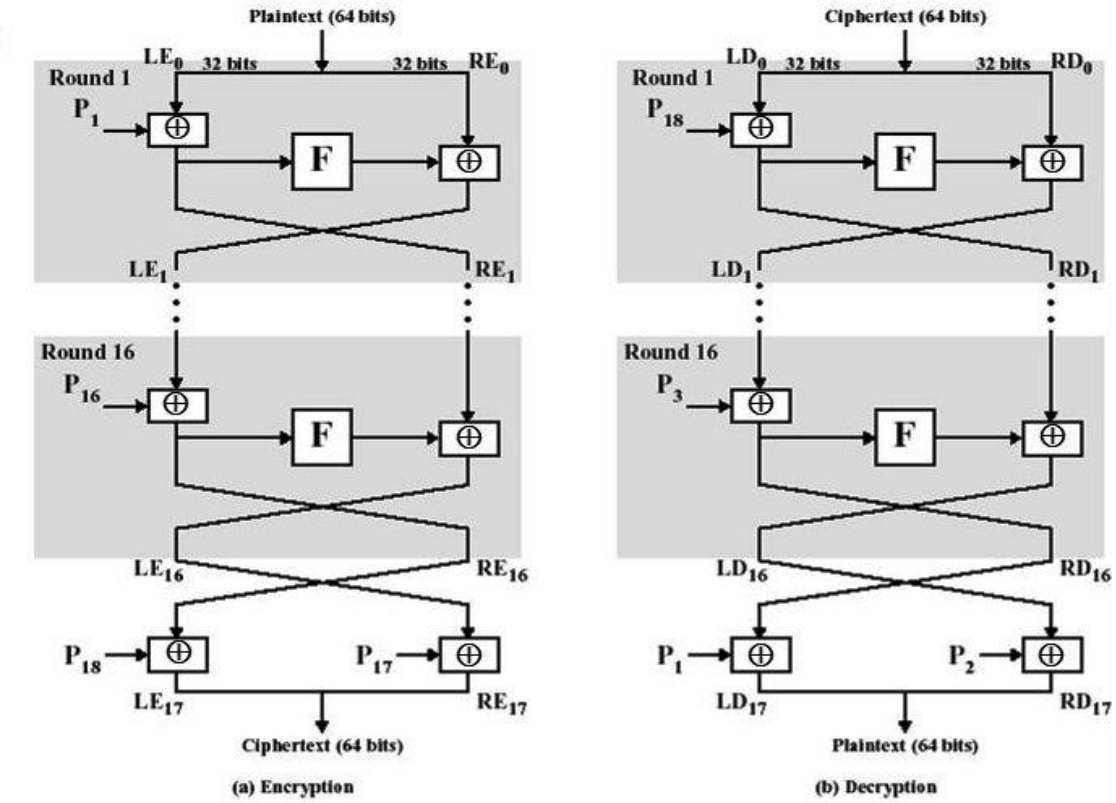

Figure 2: Blowfish encryption and decryption algorithm.

Advanced Encryption Standard (AES)

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length, Jens-Matthias B. et al (2013). During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text Gurjeevan, S. et al (2011). AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an Add Round Key stage. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation Zilhaz, J. C. *et al.*, (2010). Figure 3 shows the over-all process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

Each round of AES is governed by the following transformations.

1. Substitute Byte transformation

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte an 8-bit substitution box which is known as RijndaelSbox.

2. Shift Rows transformation

It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, is cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

3. Mix-columns transformation

This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

4. Add round key transformation

It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse**.**

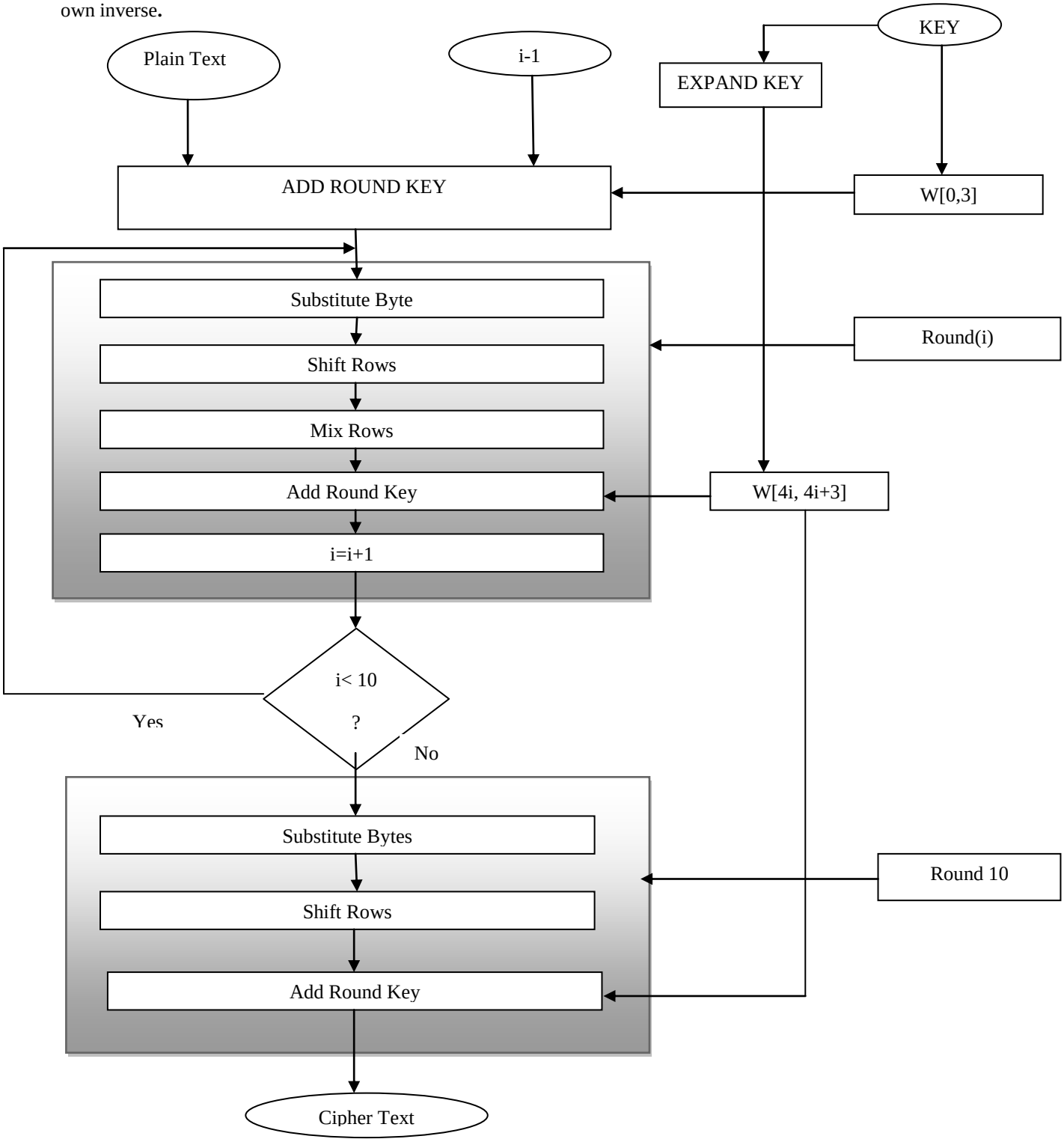

Figure 3: Advanced Encryption Standard (AES) Algorithm

System Architecture

The architecture of the system design is 3-tier. The tiers are presentation tier, middle tier and data tier. The presentation tier is the user interface and it is designed using HTML. The middle tier connects the presentation tier and the data tier together. The middle tier is also called the business logic. It was designed using C#.net and it runs on the local server. The data tier (database) is the part of the system that is responsible for storing the data. The database management system used for developing this system is MYSQL database. Figure 7 below shows the System Architecture of the proposed security model to enhance the security of data stored in cloud using AES, Blowfish algorithm and SMS.

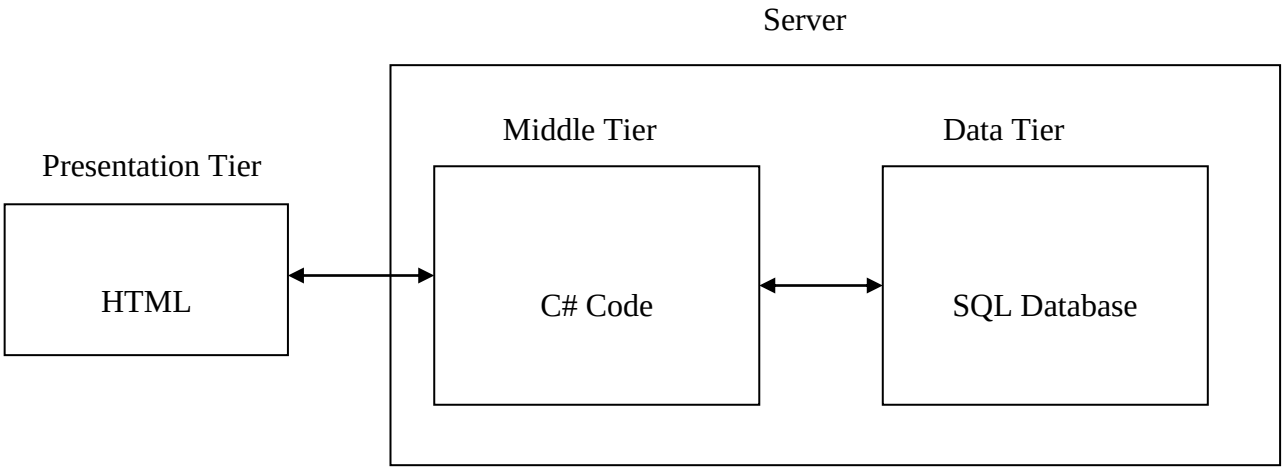

Figure 4 System architecture

Expected Results

Implementation of the new security model for cloud computing environment has been done using Visual Studio IDE. Visual Studio is an IDE in which developers work when creating programs in one of many languages, including C#, for the .NET Framework. It is used to create console and graphical user interface (GUI) applications along with Windows Forms or WPF (Windows Presentation Foundation) applications, web applications, and web services in both native code together with managed code for all platforms supported by Microsoft Windows, Windows Mobile, .NET Framework, .NET Compact Framework and Microsoft Silver light. The developed application produces physical results. These results are the outcome or outputs of the application which are in accordance with the requirement of the system. The outcome or outputs of the application are presented below with each output carrying its title that explains what it does in the developed system.

Figure 5 shows the login screen of the developed security framework. The page enables the polytechnic registrar or the designated officer to login and upload data to cloud. If the username and password entered by the designated officer are valid, the software will open the main page where the designated officer will securely upload and download files. On the other hand, if an authorized user enters an invalid password, a message will be sent to the designated officer's account informing him of someone trying to gain access to his account.

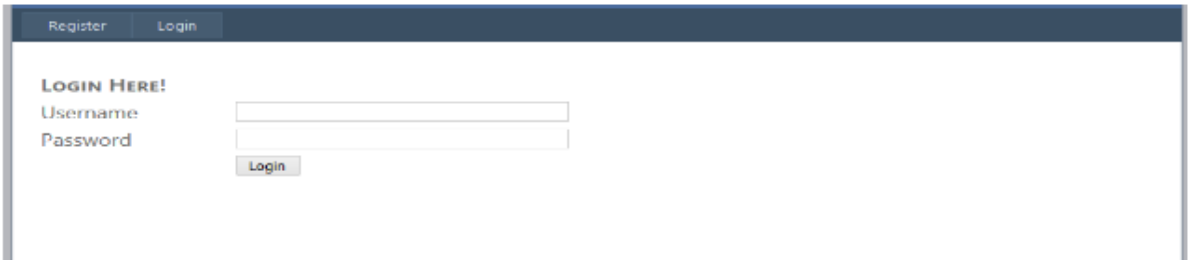

Figure 5: login Screen

If the designated officer is successfully authenticated, he is redirected to Figure 6 (file upload page) where he can upload and download data. In the upload files section, the designated officer uploads a file by first clicking on the browse button to select a text file. After selecting the desired file, he then clicks on the upload button to have his file stored to the cloud

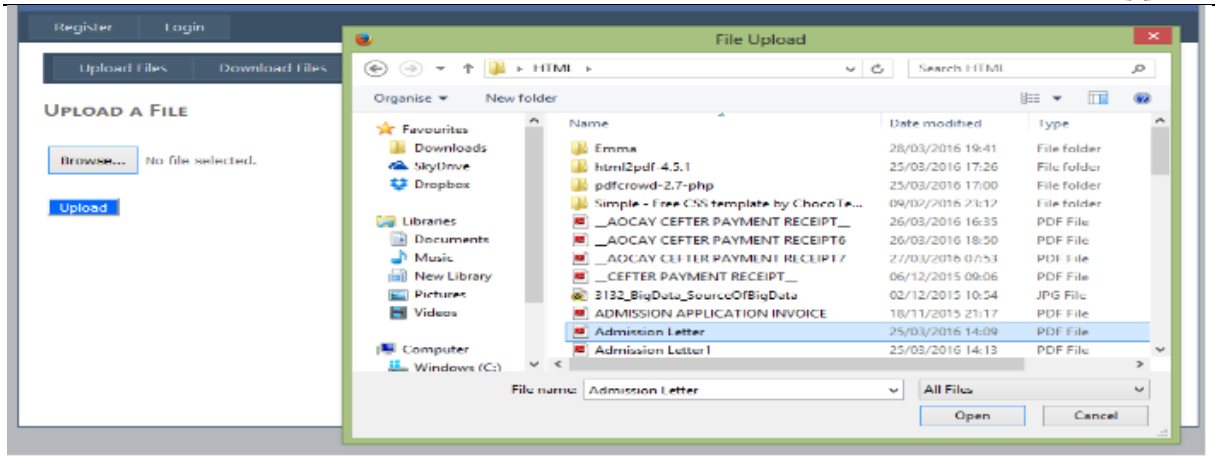

Figure 6 File upload

Figure 7 shows encrypted files stored in the cloud. If an authorized or unauthorized user tries accessing any of these files, a message is displayed which shows that the file could not be opened because it is either not a supported file type or because the file has been damaged (for example, it was sent as an email attachment and wasn't correctly decoded). These files can only be opened after proper decryption

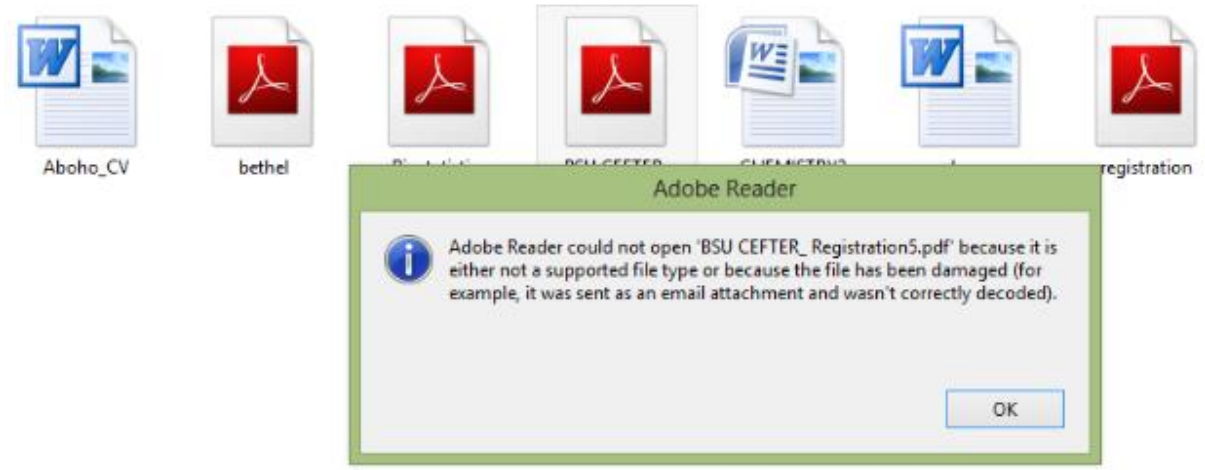

Figure 7: Encrypted files

In this paper the problem of information insecurity in the polytechnic analyzed and addressed once and for all. The proposed security model provides a mechanism that allows the polytechnic management to handle the privacy and integrity of their information stored in the cloud without relying on the credibility of the cloud provider. The new security application utilized two cryptographic algorithms, namely: AES, Blowfish encryption and SMS verification in cloud computing to provide a tight security which will protect data stored in cloud as well as enable access to data only on successful authentication and verification.

Acknowledgement

I wish to sincerely acknowledge the Nigerian Government Agency, (TETFUND) Tertiary Education Trust Fund for funding this research work.

References

[1]. Arijit U., Debasish J., and Ajanta D. (2013) "A Security Framework in Cloud Computing Infrastructure". International Journal of Network Security & Its Applications, 5(5), pp 11-24.
[2]. Deepika V. and Karan M. (2014). "To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms." International Journal of Advances in Science and Technology, 2(4), pp 41-44.
[3]. Jens-Matthias B., Nils G., Meiko J., Luigi L., and Ninja M. (2013). "Security and Privacy Enhancing Multicloud Architectures". IEEE Transactions on Dependable and Secure Computing, 10(4), pp 212-224.
[4]. Kangchan L., (2012). "Security Threats in Cloud Computing Environments." International Journal of Security and Its Applications 6(4), pp 25-32.
[5]. Keiko H., David G., Eduardo F. and Eduardo B. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications, 3(4), pp 1-13. (2013).
[6]. Gurjeevan, S., Ashwani, S. and Sandha, K. S. (2011) "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System," *International Journal of Multi-disciplinary Research*, 1(4), pp. 143-151.
[7]. Manoj K. and Kranti A. (2014). "Use of Digital Signature Standard with Station to Station Key Exchange Agreement and Cloud Manager to Enhance Security in Cloud Computing." International Journal of Applied Information Systems, 7(8), pp 1-5.
[8]. Manish, M., Dhote, C., Deepark, H. (2013). "Clod Computing Risk, Threats, Vulnerability and Controls: A Survey" International Journal of Computer Applications. Volume 67- No.3 pp 978.
[9]. Mohammed, A., Eric, B. and James, A. (2012). "Cloud Computing Security: From Single to Multi-Clouds." Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS), Institute of Electrical and Electronics Engineers, pp 5490-5499.
[10]. Nithya, C., Pethuru, R., Thenmozhi, K. and Rengarajan, A. (2016). "Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique."*International Journal of Digital Multimedia Broadcasting*, Volume 2016, Article ID 8789397, pp 1-6
[11]. Ranjit K. and Raminder, P. S. (2015). "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques."*International Journal of Mobile Computing & Application*, 2(3), pp 38-44.
[12]. Saikumar, M. and Vasanth, K. (2015) "Blowfish Encryption Algorithm for Information Security." *ARPN Journal of Engineering and Applied Sciences*, 10(10), 4717-4719.
[13]. SatarupaB., and Abhishek M. (2013). "A Survey on Data Security in Cloud Computing: Issues and Mitigation Techniques." International Journal of Research in Engineering and Technology, 2(2), pp 26-30.
[14]. Sudhansu R. L. and Biswaranjan N. (2014). "Enhancing Data Security in Cloud Computing Using RSA Encryption andMD5 Algorithm." *International Journal of Computer Science Trends and Technology (IJCST)*, 2(3), pp 60-64
[15]. Sumita, L. and AjayK.(2014). "An Approach for Ensuring Security in Cloud Environment." *International Journal of Advances in Computer Science and Technology*, 3(2), pp 92-95.
[16]. Zilhaz, J. C., Davar, P. and Nishantha, G. G. D. (2010) "AES and Confidentiality from the Inside Out," *the 12th International Conference on Advanced Communication Technology (ICACT)*, pp. 1587-1591.