Computer Engineering and Applications Vol. 10, No. 1, February 2021

A Computer Security System for Cloud Computing Based on Encryption Technique

Aliu Daniel[1], Saliu Mohammed Shaba[2], Muyideen Omuya Momoh[3], Pascal Uchenna Chinedu[1], Wilson Nwankwo[4]

[1]*Department of Electrical and Computer Engineering, Edo University Iyamho, Nigeria*
[2]*Federal College of Freshwater Fisheries Technology, New Buss, Nigeria*
[3]*Faculty of Air Engineering, Air Force Institute of Technology Kaduna, Nigeria*
[4]*Department of Computer Science, Edo University Iyamho, Nigeria*
**aliu.daniel@edouniversity.edu.ng*

ABSTRACT

In recent years, progressively data proprietors have embraced cloud storage service, by which they will subcontract their data to the cloud server to significantly reduce the local storage overhead, due to the rapid growth in the cloud computing market and development. Cloud computing is the delivery of hosting services that are provided to clients over the web. It is quite common, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that may be rapidly provisioned and released with minimal management effort or service provider interaction. Sensitive information on the cloud is developing unexpectedly and bringing up several challenges and massive security concerns of the modern-day world. The cloud data and services reside in massively scalable data centers and may be accessed ubiquitously. Some issues concern in accessing this data is the security and confidentiality of consumer data in phrases of its location, relocation, availability, and security. Numerous users are surfing the Cloud for various purposes, therefore, they have highly safe and protracted services. The long run of the cloud, especially in expanding the range of applications, involves away the deeper degree of privacy, and authentication. Because of the safety concern associated with cloud computing, this paper presents a Computer Security System for Cloud Computing by employing a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) technique before it is launched to the cloud, thus ensuring data confidentiality and security which is implemented with packet tracer.

Keywords: Cloud Security, Cloud Computing, Delivery Models Security, Cloud Threats, Cloud vulnerabilities

1. INTRODUCTION

The conventional inner information systems, which require continuous investments, are turning much less pleasing to the organization, while on-demand information technological know-how offerings primarily based on cloud computing are increasingly more turning into prominent [1]. The touchy data is stored in the interior data center in the conventional interior information system, which is protected by the organization. Cloud migration connotes

that the organization will lose the right to manage information security. Data is the foundation for the existence of an organization, and the loss of control over data results in larger protection dangers than the common inner information systems [2]. Cloud computing is network-based surroundings that specialize in sharing computation resources. Cloud sources are supplied to customers as a service on a required basis. Resources in Cloud Systems can be pooled amongst an outsized number of users, and to a house with increased load, the system may want to improve its potential correctly via including extra hardware [3]. Cloud computing allows users to create, configure, and customize applications online. Cloud computing goals to offer computing power, storage, and software program such as infrastructure on demand and leverages on recent practical sciences inclusive of the Internet to provide services to customers [4],[5]. According to the National Institute of Standard and Technology (NIST), Cloud architecture has three basic models of deployment private, public, and hybrid cloud [6]. The private cloud infrastructure is built, owned, and control by an organization [6]. The public cloud infrastructure is rendered to an organization requiring services and is own by Cloud Serve Provider (CSP) [5]. The hybrid is an arrangement of Private and Public Cloud models together [5]. For users in the cloud to expediting access to cloud services, three services are made available such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [7]. All these services are all deployed by small, medium and larger Industries. These services speedily allow the customers to store and access data remotely [7]

Despite the numerous merits, cloud storage unavoidably suffers from some security challenges [8]. Primarily, internal attackers and the external attackers (e.g, hackers) might try to get some classified information from the outsourced data which can lead to privacy exposure [8]. Also, the paper dwells on the fact that cloud computing has become a social phenomenon used by most people every day. As with every important social phenomenon, there are critical issues that limit its widespread adoption such as data confidentiality, data integrity, data deletion, and data authentication.

Most issues start from the fact that the customer loses control of his or her data because it is stored on a computer belonging to someone else (the cloud provider). This happens when the owner of the remote servers is a person or organization other than the user; as their interests may point in different directions (for example, the user may wish that his or her information is kept private, but the owner of the remote servers may want to take advantage of it for their interest). For a user to have some level of confidence in the hosted data there is a need to encrypt the data before outsourcing the data to the cloud. Given these, a Computer Security System for Cloud Computing by employing a simple data protection model, where data are encrypted using Advanced Encryption Standard (AES) technique before it is launched to the cloud, by ensuring data confidentiality and eliminate the concerns regarding data privacy is implemented with Packet Tracer.

2. LITERATURE REVIEW

This section comprises two sub-parts. The first sub-part deals with the overview of fundamental concepts that are pertinent to cloud computing are discussed. The second sub-part covers the review of similar works that are critical to this paper.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

2.1. OVERVIEW OF CLOUD COMPUTING

Cloud computing is the concept implemented to decipher the daily computing problems [9]. Cloud computing is a virtual pool of resources and it provides these resources to users via the internet [9]. Cloud computing is internet-based development and used in computer technology. It can be expended through web Brower or via a distinct API [7]. Figure 1 depicts the structure explanation of Cloud [7]. The prevalent problem associated with cloud computing is data privacy, security, and reliability, etc. But the most important between them is security and how cloud provider assures it [9]. In this paper, the proposed work plan is to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in the cloud as per the different perspectives of cloud customers. Encryption is a well-known technology for protecting sensitive data. The combination of Public and Private Keys encryption to hide sensitive data of users and ciphertext retrieval is quite common with this technique. Figure 1 depicts a usual cloud-primarily based state of affairs that consists of the cloud service provider and the cloud customers in a cloud computing architecture. The reason for the illustration is to set up the arrangement that makes the thought of cloud computing a concrete one. The community structure is self-explanatory with the identification of cloud customers when viewed in-line with the dialogue of the cloud computing thinking introduced earlier.

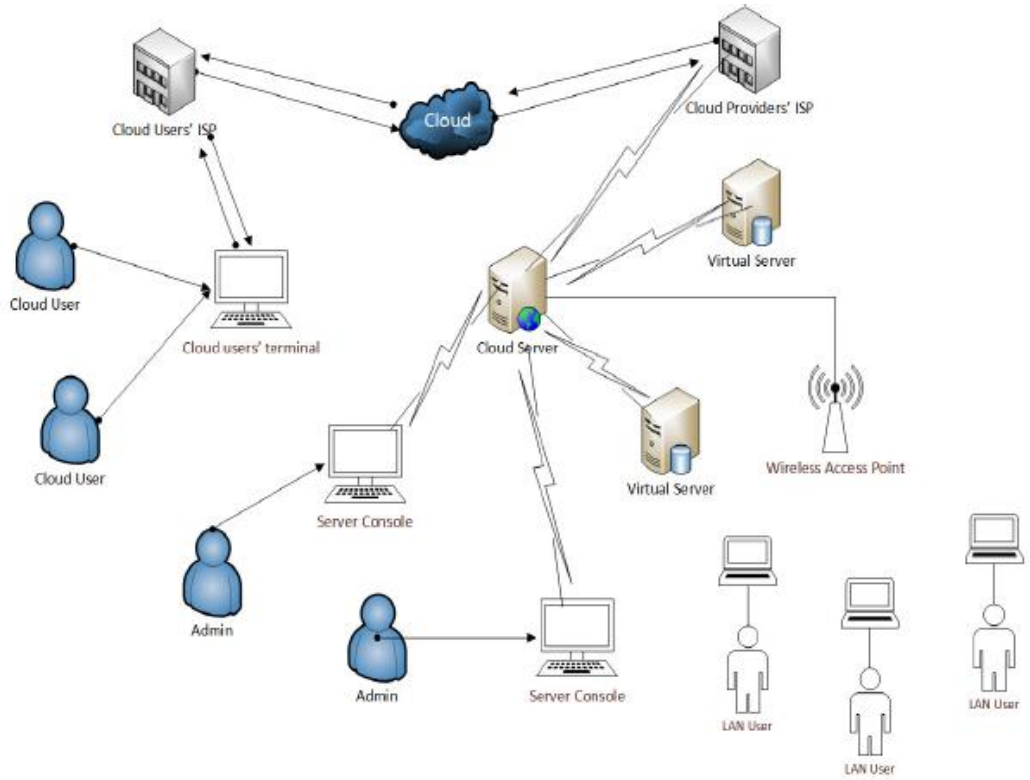

FIGURE 1. A Classic Cloud Structure [10]

Figure 2 denotes the categorized organization based on which a cloud is observed in the form of IaaS, PaaS, and SaaS from any cloud end-user viewpoint. As illustrated in Figure 2, the technical details, preparations, and administration of the

cloud service providers' community is obvious to the cloud user. From the cease of the cloud user, the service from the issuer comes in the shape of SaaS, PaaS, or IaaS the place the cloud customer has no intention or fear about what goes on in the interior organization of the cloud provider providers' network.

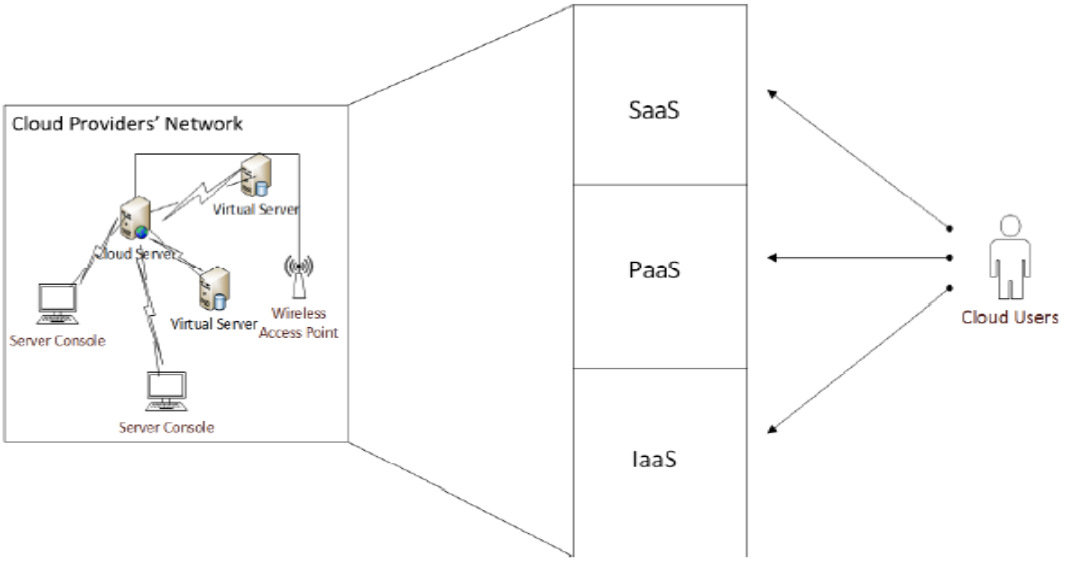

FIGURE 2. Cloud Service Hierarchy [10]

2.1.1 SECURITY IN CLOUD COMPUTING

If we wish to enable cloud-driven growth and innovation through security, we must have a clear framing on what is meant by security. Security has been hard to define in the general. The canonical goals of information security are Confidentiality, Integrity, and Availability. A few examples of how they can be supported by both technical and non-technical mechanisms are discussed as follows [11]:

I. Confidentiality refers to keeping data private. Confidentiality is supported by technical tools such as encryption and access control, as well as legal protections.

II. **Integrity** is a degree of confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. Integrity is supported by well-audited code, well-designed distributed systems, and robust access control mechanisms.

III. **Availability** means being able to use the system as anticipated. Availability is supported by capacity building and good architecture as well as well-defined contracts and terms of the agreement.

IV. Accountability maps actions in the system to responsible parties. Accountability is supported by robust identity, authentication, and access control, as well as the ability to log transactions and then, critically, audit these logs.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

V. Assurance refers to the need for a system to behave as expected. Assurance is supported by a trusted computing architecture in the cloud, and by careful processes mapping from business case to technical details to legal agreements.

VI. Resilience in a system allows it to cope with security threats, rather than failing critically. Resilience is supported by redundancy, diversification, and real-time forensic capacity.

2.1.2. BASIC SECURITY ALGORITHM

Many organizations and users store their important data on the cloud and data is also accessed by numerous users, so it is imperative to secure the data from intruders. To provide security to the cloud many algorithms are designed for the function. Security Algorithms are classified basically as follows [9]:

1. Private Key (Symmetric) Algorithms: Use a single secret key for encrypting a large amount of data and have fast processing speed. These algorithms use a single secret key that is known to the sender and the receiver. RC6, DES, Blowfish, 3DES, AES are some prime examples of these algorithms [12]. Also, the advantages and disadvantages of AES are in [13].
2. Public Key (Asymmetric) Algorithms: Use a key pair for a cryptographic process, with a public key for encryption and a private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public-key algorithms [14]. The basic existing security algorithms such as BlowFish Algorithm, DES, AES, and RSA are discussed in [9], [14], [12].

2.1.3. COMPARING AES WITH OTHER ALGORITHMS

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, the nonlinearity of the key expansion practically eliminates the possibility of equivalent keys in AES. A performance comparison amongst AES, DES, and Triple DES for different microcontrollers shows that AES has a computer cost of the same order as required for Triple DES. Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES, and RC2 in terms of execution time (in milliseconds) with different packet sizes and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has an advantage over RC2, RC6, and Blowfish in terms of time consumption [15].

System can be increased using AES Encryption algorithms, when using keys as 128 bit AES, determining the private key is not possible even if the attacker attacks the data on transit or storage [16]. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Encryption algorithms play an important role in data security on the cloud and by comparison of different parameters used in algorithms, it has been found that the AES algorithm uses the least time to execute cloud data [16]. Blowfish algorithm has the least memory requirement. DES

algorithm consumes the least encryption time. RSA consumes the longest memory size and encryption time. AES has its overall advantages of being a reliable, fast, secured, and safe system over others. The following are the Features of the AES Encryption Algorithm [15], [12]:

I. AES algorithm works on the principle of Substitution Permutation network.

II. AES does not use a Feistel network and is fast in both software and hardware.

III. AES operates on a 4X4 matrix of bytes termed as a state

IV. The AES cipher is specified as several repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext.

V. Each round consists of several processing steps, including one that depends on the Encryption key.

VI. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TABLE 1
Comparison of Encryption Standards based upon Different Factors [16]

Factors	DES	3DES	RC6	Blow fish	AES
Key size	56 Bits	168 Bits	128, 192 or 256 Bits	32-448 Bits	128, 192, or 256 Bits
Block size	64 Bits	64 Bits	128 Bits	64 Bits	128, 192 or 256 Bits
Cipher type	Block cipher	Block cipher	Symmetric algorithm	Symmetric block cipher	Symmetric cipher algorithm
Keys	Private key	Private key	Single key	Private key	Private key
Attacks	Vulnerable to differential and linear	Vulnerable to differential, Brute force attacks	Vulnerable to differential, Brute force attacks	Vulnerable to differential, Brute force attacks	Strong against differential, Brute, Linear force attacks
Security	Proven inadequate	Inadequate	Vulnerable	Less secure	Consider secure

2.1.4. EVALUATION OF TOOLS: PROS AND CONS OF CLOUD COMPUTING

Pros of cloud computing [15]:

I. **No cost on infrastructure:** Cloud computing is divided into 3 major categories as per their services like IaaS, PaaS, SaaS. In all these categories, one thing is common that you don't need to invest in hardware or any infrastructure. In general, every organization has to spend a lot on its IT infrastructure to set up and hire a specialized team. Servers, network devices, ISP connections, storage, and software – these are the major things on which you need to invest if we talk about General IT

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

infrastructure. But if you move to cloud computing services, then you don't need to invest in these. You just go to the cloud services provider and buy the cloud service.

II. **Minimum management and cost:** Since one doesn't need to invest in the infrastructure, the cost of managing it is also saved. As for IT infrastructure, one needs to hire qualified staff to manage it. While on the cloud, the management of its infrastructure is sole of the cloud provider and not of the cloud user thus again cost saving

III. **Forget about administrative or management hassles:** Whenever there is a purchase or up-gradation of hardware, a lot of time is wasted looking for the best vendors, inviting quotations, negotiating rates, taking approvals, generating POs and waiting for delivery, and then in setting up the infrastructure. This whole process includes lots of administrative/managerial tasks that waste a lot of time. While in cloud services, you just need to compare the best cloud service providers and their plans and buy from the one that matches your requirement. And this whole process doesn't take much time and saves lots of effort. Your maintenance tasks are also eliminated in the cloud.

IV. **Accessibility and pay per use:** Cloud resources are easily accessible from around the globe – anytime, anywhere and from any device and you have complete access to your resources. This decides your billing also you only pay for what you use and how much you use. It's like your phone or electricity bill. But on other IT infrastructure, one spends the complete amount in one go and it is very rare that those resources are used optimally and thus the investment goes waste.

V. **Reliability:** Your infrastructure in the cloud increases the reliability and availability of applications and services. Cloud services run on pooled and redundant infrastructure which provides you with higher availability of your services.

Cons of cloud computing [12]**:**

I. **Requires good speed internet with good bandwidth:** To access your cloud services, you need to have a good internet connection always with good bandwidth to upload/download files from/to the cloud.

II. **Limited control on infrastructure:** Since you are not the owner of the infrastructure of the cloud, hence you don't have or have limited access/control on cloud infrastructure.

III. **Restricted or limited flexibility:** Although the cloud provides a huge list of services but consuming them comes with a lot of restrictions and limited flexibility for your applications or developments.

IV. **Ongoing costs:** Though you can save your cost of spending on the whole infrastructure and its management, on the cloud you need to keep paying for services as long as you use them. But in traditional methods, you only need to invest once.

V. **Security:** Security of data is a big concern for everyone. Since cloud services are public hence it depends on the provider as to how they are taking care of your data.

So, before opting for cloud services, it is required that you find a provider who follows max compliances for data security.

3. REVIEW OF RELATED WORKS

The pertinent challenges of this paper are centered on cloud computing data security as it relate to the following literatures. [17] Worked over public cloud infrastructure and proposed a model that is well suited for preserving the integrity with the help of cryptographic primitives. This technique is purely based on cryptographic storage services. In the proposed procedure, when a user wants to send data to other users, they first generate a master key that encrypts their message. The secret key for decryption is stored on the receivers' system for decrypting the same message. They use the concept of index encryption and tokens are generated with the knowledge of the secret key. But the searching method is not very efficient for encrypted data. They discussed Symmetric Searchable Encryption (SSE) and Asymmetric Searchable Encryption (ASE). Although these techniques are used for encrypted data searching it increases complexity and makes the system cumbersome. [18] Worked on different security aspects in computing, the technique provided a new way to authenticate in 3-dimensional approaches. It provided availability of data by surmounting many existing problems like denial of services and data leakage etc. Additionally, it also provides more flexibility and capability to meet the rising demand of today's complex and diverse network. But in this model, the data stored is not in encrypted form and once the username and password are lost, the data can easily be retrieved by any unauthorized user. [19] Discussed on after subcontracting data to a cloud service provider, the organization will have challenges in unswervingly monitoring information security. However, for the organization, not all information requires equal stages of safety

Ref [20] proposed a system to achieve secure data sharing for dynamic groups in the cloud, they expect to combine the group signature and dynamic broadcast encryption techniques. Unfortunately, each user had to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the ciphertext increase with the number of revoked users. [21] Worked on Data Security Challenges and Its Solutions in Cloud Computing where the authors discussed several data security challenges and proposed some solutions. Some components of data protection ranging from the use of the application, storage, and network were discussed. [22] Categorised cloud protection challenges into data storage concerns, identity administration & get right of entry to control, contractual and legal issues. The troubles are further categorised into Data storage issues: Data privacy and integrity, data recovery and vulnerability, flawed media sanitization and records backup. Identity administration and access control: malicious insider and outdoor intruder. Contractual and Legal issues, Service Level Agreements (SLAs), and criminal issues.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

4. DEVELOPMENT AND IMPLEMENTATION OF THE PROPOSED SYSTEM

In the proposed system, the emphasis was based on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used the alphabet for ciphertext. In the proposed algorithm, initially, the plain text is converted into the corresponding ASCII code value of each alphabet. Furthermore, in the proposed algorithm, key-value ranges between 1 to 128, 192, and 256. The algorithm is used to encrypt the data of the user in the clouds. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user. The proposed algorithm is described in details as follows:

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. AES with 128-bit key length was used. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical. The 16-byte encryption key, in the form of 4-byte words, is expanded into a key schedule consisting of 44 4-byte words. The 4 X 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, the input state is XORed with the first four words of the schedule.

4.1.1. ENCRYPTION PHASE

In the encryption phase each round consists of the following four steps:

I. SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).

II. ShiftRows – a transposition step where each row of the state is shifted cyclically a certain number of times

III. MixColumns – a mixing operation that operates on the columns of the state, combining the four bytes in each column.

IV. AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule

Figure 3 shows the system flows from the web input, the processing and, series of the procedure to encrypt the information (process), view the messages, data, or graphics, and finally save the program for future use. Figure 4 depicts the program flow chart of the implementation of the system,

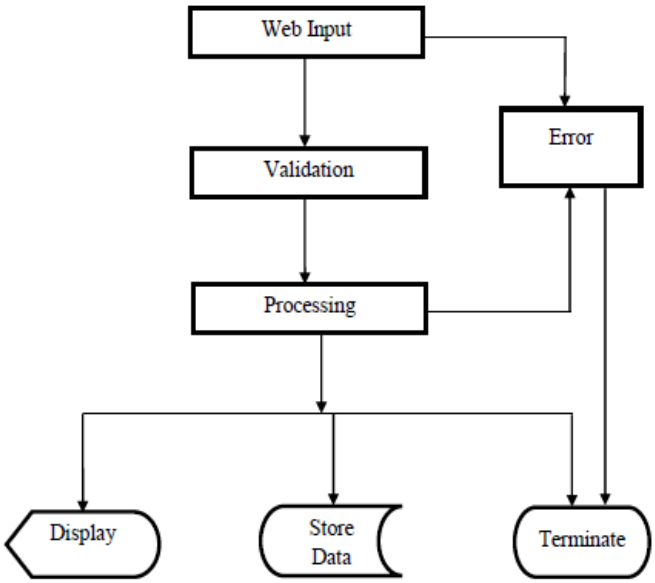

FIGURE 3. System Flow Chart

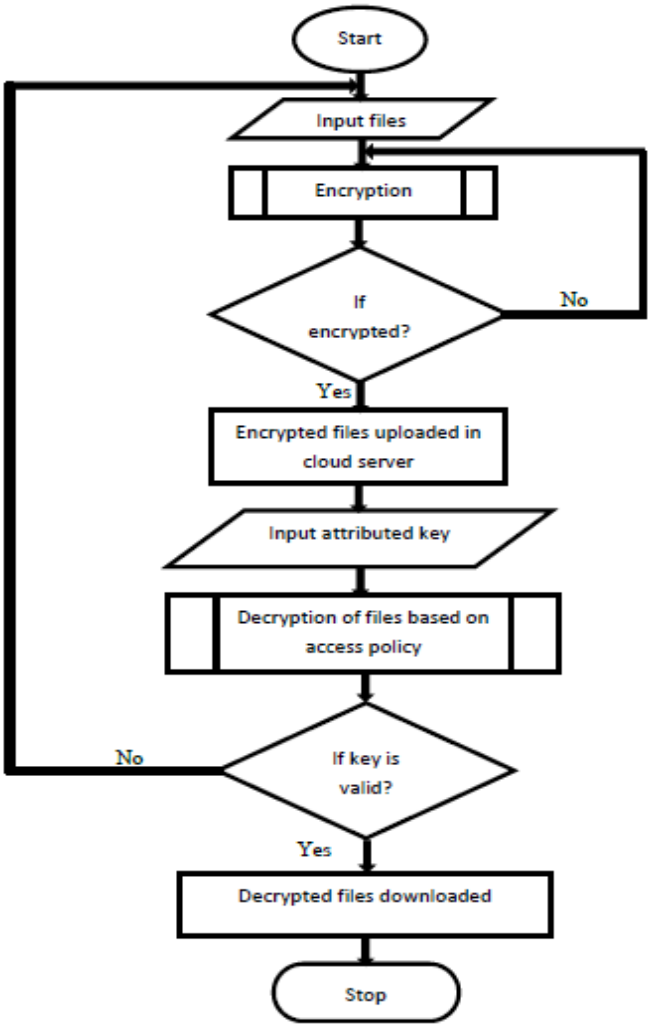

FIGURE 4. Program Flow Chart

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

4.1.2. TEST RUN OF THE SYSTEM

The testing of the system was carried out by executing the program on a computer system; Packet Tracer was used for designing and configuring the cloud computing security system. The purpose of this test run is as follows:

I) To check if there are any bugs in the system.

II) To check the effectiveness and efficient operations of the system.

II) To check and make sure that the new system meets the organization or user requirements.

Figure 5 shows the interface view of the design of the cloud security system together with the various components used to achieve the design of the system.

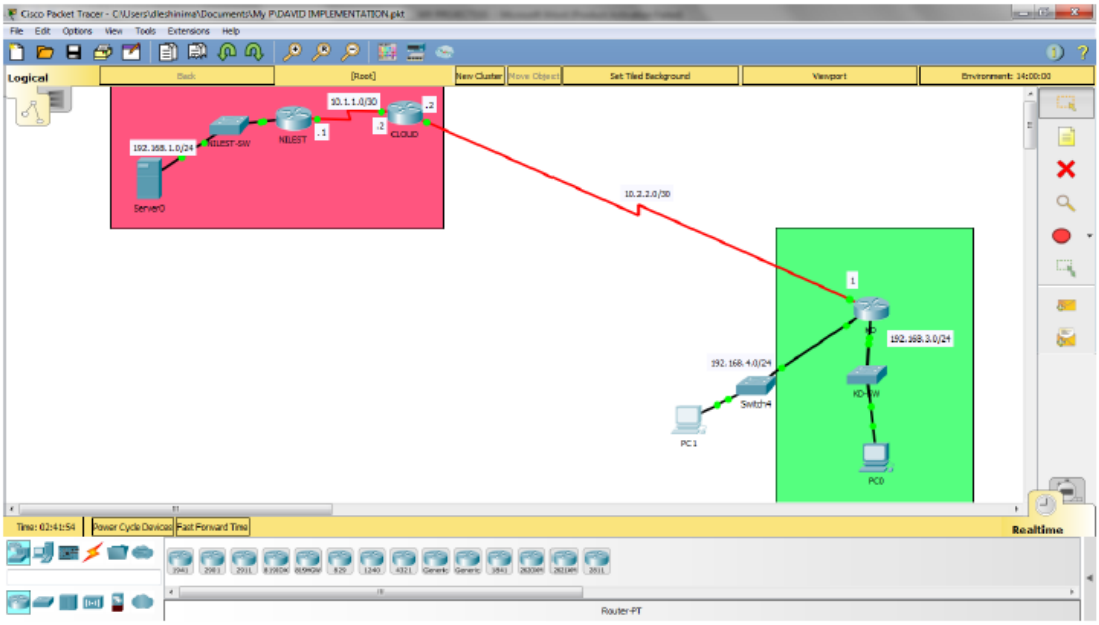

FIGURE 5. Interface Form

Figure 6 shows the transmission of packets from the client personal computer (PC) to and fro the internet.

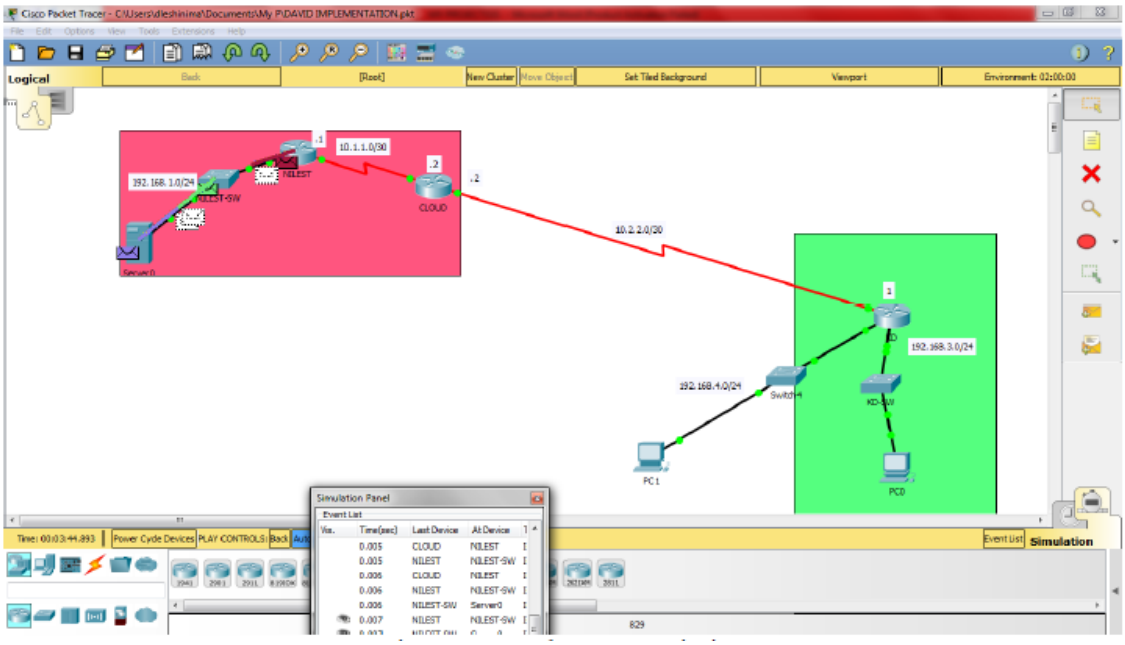

FIGURE 6. Packets transmission

5. CONCLUSION

It concluded that the AES-128 bits encryption algorithm was chosen to be the choice of this research material using in communication. This is because the AES algorithm is updated time by time and it has already been used by U. S. Government Standard encryption algorithm for encrypting electronic information and replacing DES and 3DES as well. Also, it is the most frequently used algorithm, compared to other types of algorithm. Apart from that, the AES algorithm had the advantage of more secure encrypted communication when compared to the other encryption algorithm. The encrypted and decrypted data is unbreakable from the beginning until today by using the AES algorithm.

Lastly, it was needed to test the accuracy of the AES algorithm in encrypting or decrypting the data, whether the plaintexts were correctly processed or not in communication between the sender and receiver, so that the information can be transferred more securely and correctly.

Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with a new problem. The identification of security challenges and mitigation techniques in a large number of services of Cloud Computing is a very challenging task. The research work indicates that Security and Privacy are the major issues that are needed to be countered, efforts are being made to develop many efficient systems that can provide security and privacy at the user level and maintain the trust and intellectual property rights of the user. A Computer Cloud Security System based on AES technique is hereby developed to address the challenges associated with cloud computing security and privacy.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

REFERENCES

[1] Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. *International Journal of Information Management, 50*, 387-394.

[2] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences, 305*, 357-383.

[3] Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access, 4*, 1375-1384.

[4] Gartner F. (2011) "A survey on security issues in service delivery models of cloud computing "Journal of Network and Computer Application. Vol. 34, Issue 1, Pp. 1-11

[5] Odun-Ayo, I., Ajayi, O., & Misra, S. (2018). Cloud computing security: Issues and developments.

[6] Tariq, M. I. (2019). Agent-Based Information Security Framework for Hybrid Cloud Computing. *KSII Transactions on Internet & Information Systems, 13*(1).

[7] Butt, S. A., Tariq, M. I., Jamal, T., Ali, A., Martinez, J. L. D., & De-La-Hoz-Franco, E. (2019). Predictive variables for agile development merging cloud computing services. *IEEE Access, 7*, 99273-99282.

[8] Yang, C., Chen, Q., & Liu, Y. (2019). Fine-grained outsourced data deletion scheme in cloud computing. *International Journal of Electronics and Information Engineering, 11*(2), 81-98.

[9] Rachna Arora & Anshu Parashar (2013) "International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul- Aug 2013, pp.1922-192619.

[10] Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications, 6*(1), 25.

[11] Vikas M. *et al* (2014), "Network Security: Security in Cloud Computing", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 1, Jan 2014 Page No. 3643-3651.

[12] Lokhande, U., & Gulve, A. (2014). Steganography using Cryptography and Pseudo random numbers. *International Journal of Computer Applications, 96*(19).

[13] Milind Mathur, et al., (2013) "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[14] Kester, Q.-A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2014). A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images based on a Generated Symmetric Key. *International Journal of Computer Applications, 94*(19), p19-27.

[15] Abha Sachdev & Mohit Bhansali (2013), "Enhancing Cloud Computing Security using AES Algorithm", *International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 201*.

[16] Kaur M. &Kaur S. (2014) "Survey of Various Encryption Techniques for Audio Data" International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4, Issue 5, May 2014. Pp. 1314-1317

[17] Kamara, S., & Lauter, K. (2010). *Cryptographic cloud storage.* Paper presented at the International Conference on Financial Cryptography and Data Security. pp 1 – 8

[18] Prasad *et al., (2013)* Software reliability measuring using modified maximum likelihood estimation and SPC "*International Journal of Computer Applications" (0975 – 8887)Volume 21– No.7, May 201.*

[19] Mircea, M. (2012). Addressing Data Security in the Cloud. *World Academy of Science, Engineering and Technology, 66*, 539-546.

[20] Sathana, V., & Shanthini, J. (2013). Three Level Security System for Dynamic Group in Cloud. International Journal of Computer Science Trends and Technology, 1(2).

[21] Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*, 204-209.

[22] Rao, B. T. (2016). A study on data storage security issues in cloud computing. *Procedia Computer Science, 92,* 128-135.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)