Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 9, September 2019, pg.245 – 257

A Review on Cloud Computing Security

Oluyinka. I. Omotosho*

Corresponding Author: O. I. Omotosho.* ***Email:* *oiomotosho@lautech.edu.ng*
Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Oyo state, Nigeria
Email*: oiomotosho@lautech.edu.ng*

I. INTRODUCTION

Cloud computing is commonly used to represent any work done on a computer, mobile or any device, where the data and possibly the application being used do not reside on the device but rather on an unspecified device elsewhere on the Internet. The basic premise of cloud computing is that consumers (individuals, industry, government, academia and so on) pay for IT services from cloud service providers (CSP). Services offered in cloud computing are generally based on three standard models (Infrastructure-as s service, Platform-as a service, and Software as a Service) defined by the National Institute of Standards and Technology (NIST). The reason for cloud existence is to resolve managing problems being faced for data that were excessively stored, either mandatory capacity was limited due to the infrastructure of the business, or large capacity that led to a wasted capital. Apart from those major factors such as the initial capital, capitals and the service-fix cost, the sophisticated effort for the patching, the managing and the upgrading of the internal infrastructure is a huge obstacle for firm's development and mobility. For many firms where client and cultural competency have not got the strength to manage large data center environments and infrastructure, it would be wise to upload their files or data backups to another machine via internet, in order to concentrate more on the organizations primary objectives.

1.1 CLOUD COMPUTING

Cloud computing is the technology or better the ability to upload and maintain data, share/trade software and hardware resources, storage via the internet. The super user of the cloud server is the cloud operator and he/she has access everywhere. Better still, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." . Many start up organizations began with function of cloud, for example applications (pinterest) that hold all of their data to cloud servers like Amazon's Cloud Platform (Amazon Web Services).

1.2 CLOUD COMPUTING SECURITY

Cloud computing security is defined as the processes, interactions and policies designed to fulfil security insurance and information protection for a cloud-based environment. It uses both logical and physical ways for the whole sharing system of the cloud like the software (SaaS), platform (PaaS) and infrastructure (IaaS). In a cloud security policy, the cloud provider sets the constraints of the end-user as he is limited to permissions (Acceptable User Policy). Cloud security policy is a mandatory procedure for every corporation and business as the level of cloud security defines whether an organization will choose to trust the network topology or

refer to another model. This cloud model is composed of five essential characteristics, three service models, and four deployment models. The five essential characteristics are as follows:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

The service models are as follows:

- Cloud Software as a Service (SaaS)—Use provider's applications over a network.
- Cloud Platform as a Service (PaaS)—Deploy customer-created applications to a cloud.
- Cloud Infrastructure as a Service (IaaS)—Rent processing, storage, network capacity, and other fundamental computing resources.

The deployment models, which can be either internally or externally implemented, are summarized in the NIST presentation as follows:

- Private cloud—Enterprise owned or leased
- Community cloud—Shared infrastructure for specific community
- Public cloud—Sold to the public, mega-scale infrastructure
- Hybrid cloud—Composition of two or more clouds

1.3 THE CLOUD

Three types of cloud currently exists, private, public and hybrid. The cloud computing security models are also categorized under these models. Cloud computing security model has three security and delivery models. The three types of cloud are explained in subsequent sections.

Private cloud:

This is a cloud platform with dedicated use for home users or special organizations. Private cloud refers to a model of cloud computing where IT services are provisioned over private IT infrastructure for the dedicated use of a single organization. A private cloud is usually managed via internal resources. The terms private cloud and virtual private cloud (VPC) are often used interchangeably.

A private cloud is implemented in a corporation's internal infrastructure data center. It is more manageable to set up security, adjusting requirements and elasticity, and provides more supervision on its application and use. Private cloud offers virtual applications, infrastructure resources with permission of the cloud vendor , that he/she is responsible to put them available for share and use. It differs from the public cloud server because all the private cloud applications and resources are controlled by the corporation itself, like intranet. Security on a private cloud server is more secure than public because it disables the exposition to external and specifies the internal access on privileged users.

Public cloud:

This is designated for public clients that can register for a low price of registration or even free and take advantage of the infrastructure (storage of data, software and etc). Companies like Alibaba, Amazon Web Services, Google Cloud Platform, IBM Cloud, Microsoft Azure, Oracle Cloud are some of the companies that offer cloud computing services.

Public cloud is a model which permits access to users via web browser interfaces. In order to have access on it users have to pay in a paying method system like the electricity prepaid metering system. In fact that does not only give profit to the cloud providers but also gives them the ability for optimization. Cloud clients then debit their IT charge at a logical level by lowering the capital loss on the IT system infrastructure. From a security perspective, public cloud are less secure according to other ones because they focus on ensuring all the applications are online than protecting the data uploaded from possible attacks. Therefore privacy and trust fade out with public clouds and their clients keen on negotiating with private cloud servers for better security results. Possible solutions for this matter would be 1) both cloud provider and client agree on sharing data responsibility in supporting daily checks and validations through their own systems. 2) for each of them to have a responsible roles for dealing with security within their permission boundaries.

Hybrid cloud:

A private cloud that can expand to manage resources of public clouds. Cloud computing service models or "offerings" can be divided into three and they support the above models:

A hybrid cloud is a private cloud that is connected on one or more outwardly services. It is basically managed on the centric system infrastructure, catered as a single service, and hold on a secure network environment. It provides to its clients virtual IT resources like public and private clouds. Hybrid cloud server's vendors give more secure data management and provide several parties access the internet with high supervision and protection. It's an open architecture that allows interfaces with other 'friendly'

systems. In other words, hybrid clouds are private cloud vendors that keen to expand and be more flexible, like a mix of both public and private.

To summarize, in deciding which of three types of cloud is to be deployed, business administrators need to consider the security aspects of the corporations architectural structure, further information on the security differences between the cloud models is essential.

1. **IaaS** – (Infrastructure as a service)
   It delivers computation, network resources, also includes servers, virtual machines, storage, load balancers and other infrastructure stack.
2. **PaaS** – (Platform as a Service)
   Provides platform, business and service tools, adds development and programming applications to IaaS, includes databases, webservers, execution frameworks/runtimes and development tools
3. **SaaS** – (Software as a service)
   Provides applications from the infrastructure of the cloud and implements them on an end-user machine (Sales force CRM, Gmail/Google Apps, Microsoft Live and etc)

1.4 Cloud Computing Service or Delivery Models

The next consideration business managers and administrators have to take is related to three cloud delivery models which includes Iaas, Saas, Paas. ''Due to the pay-per-use economy model that pertains to Cloud delivery models, the degree of information security is directed towards adhering to industry standards and legislations among cloud shareholders''(Ramgovind et al. 2010).

Infrastructure as a service (IaaS)

This is a "layer" of cloud computing system that allows dedicated resources of the cloud server/vendor to be used and shared by its number of client for a price. This means that the cost of initial capital in computer hardware, servers, processors, networking devices is automatically reduced. They also give the ability to the clients of using different ways for their financial and functional requirements that other data centers cannot offer, because in a cloud system there is much more flexibility and cost effectiveness in adding or removing hardware resources. However, managers and administrators have to pay attention on unceremonious metabolisms of operational expense increase.

Software as a Service (SaaS)

This is a virtualized layer of the cloud computing system that gives the ability to clients to pay for their membership to use software applications for their vendor. This is performed by accessing through a login system via a web browser. Software's limitation and core functionality is managed according to the billing arrangement of each client. The SaaS providers can place their software on their own data centers or they can use the previews model and share it through an external IaaS vendor. The availability of IaaS services is the main factor of the SaaS model. Web browser and internet security is mandatory as the SaaS applications are accessed from it. "Web Services (WS)security, Extendable Markup Language (XML)encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the internet" (Ramgovind *et al*. 2010).

Platform as a Service (PaaS)

This layer is similar to the functionalities of the IaaS but it provides an additional pay-per-use function. The use of virtual machines in this model is a bad factor because they have to protect them against hacking activities, attacks and malware. Therefore, maintaining the applications as also enforcing the security on data forensics and authentication checks during transactions is necessary and costly.

II. CLOUD ALGORITHM (CRYPTOGRAPHIC ALGORITHMS)

This is the study of techniques for ensuring the secrecy and/or authenticity of information. The three main cryptographic algorithms are: Symmetric-Key Algorithm, Asymmetric-Key Algorithm and Hashing Algorithms.

- Symmetric-Key Algorithm Also Known as Secret Key Encryption: A single key is used for both encryption and decryption. The key, in practice, represents a shared secret between two or more communicating parties for secure communication. A few of the well-known symmetric encryption algorithms include Data Encryption Standard (DES), AES, Blowfish and Skipjack
- Asymmetric-Key Algorithm or Public-Key Encryption: The asymmetric-key algorithm or public-key encryption utilizes a pair of keys—public key and private key. The public key can be revealed, but, to protect the data, the private key must be concealed. Additionally, encryption and decryption of the data must be done by the associated private and public keys. For instance, data encrypted by the private key must be decrypted by the public key and vice versa. Some of the common examples of this algorithm are RSA (Rivest-Shamir-Adleman), Diffie–Hellman key exchange, and elliptic curve techniques.
- Hashing Algorithms, Also Called One-Way Encryption: Hashing algorithms, also called one-way encryption are algorithms that in some sense use no key. It is a vital information security tool and is used to authenticate messages, digital signatures and documents. A hash function accepts a variable-length block of data as input and produces a fixed-length hash value called message digest. Having a message digest, it is impossible to recover or find the original string. Some examples of hashing algorithms are: MD5,

SHA-1 SHA-2, and SHA-3. The primary purpose of encryption is to ensure the confidentiality of the data stored on a specific device or transmitted via the internet. While hash function ensures data integrity, any change in the original message, however small, must cause a change in the digest, and, for any given file and digest, it must be infeasible for a forger to create a different file with the same digest

EXISTING ALGORITHMS

Many organizations and people store their important data on cloud and data is also accessed by many persons, so it is very important to secure the data from intruders. To provide security to cloud many algorithms are designed. Some popular algorithms are:-

a). Data Encryption Standard (DES): This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher.

```
Algorithm:
function DES_Encrypt (M, K)
 where M = (L, R)
 M←IP (M)
 For round←1 to 16 do
 K←SK (K, round)
 L←L xor F(R,Ki)
swap(L, R)
end
swap (L, R)
M←IP-1(M)     return M
End
```

b). Advance Encryption Algorithm (AES): Advanced Encryption Standard is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES Encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

c)**. Triple- DES (TDES):** This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.

```
Algorithm:
For j = 1 to 3
 {
Cj,0= IVj
 For i = 1 to nj
 {
Cji = EKEY3(DKEY2 (EKEY1 (Pj, iCj, i-1)))
 Output Cj, i
 }
 }
```

d). Blowfish Algorithm: This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption.

```
Algorithm:
Divide x into two 32-bit halves: xL , xR
 For i = 1to 16:
 x L = xL XOR Pi
 x R = F(xL) XOR xR
 Swap  xL  and  xR
Next i
Swap xL and xR (Undo the last swap.)
```


x R = xR XOR P17
x L = xL XOR P18
Recombine xR and xL

e). IDEA: International Data Encryption Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits. IDEA consists of 8.5 rounds. All rounds are similar except the one. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. Now basic operations modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Total number of keys used for performing different rounds is 52. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the first 16 bits of the original key and K2 has the next 16 bits similarly for K3, K4, K5 and K6. Therefore for round 1 (16*6=96) 96 bits of original cipher key is used.

f). Homomorphic Encryption: Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key. In mathematics homomorphic means conversion of one data set to another, without losing its relation between them. In homomorpic, complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

g). RSA: This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption.

Algorithm

Key Generation: KeyGen(p, q)

Input: Two large primes –p, q

Compute n = p. q

$\varphi(n) = (p-1)(q-1)$

Choose e such that $\gcd(e, \varphi(n)) = 1$

Determine d such that $e.d \equiv 1 \bmod \varphi(n)$

Key:

Public key = (e, n)

Secret key= (d, n)

h). Diffie- Hellman Key Exchange: Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communication using a symmetric key cipher.

2.3 CHALLENGES OF ADOPTION OF CLOUD COMPUTING

Adoption of cloud computing can be faced by so many challenges ranging from trust to security and many more. It could also be legal and compliance challenges and organizational challenges (Andrei, 2009, Buyya *et al*., 2008, Catteddu and Hogben, 2009, Khajeh-Hosseini *et al.*, 2010). Linked to all these challenges is the issue of trust between clients and vendors, because cloud computing calls for organizations to trust vendors with the management of their IT resources and data (Shimba, 2010). Of all the challenges, security has received more mention. This is because "security is both a feeling and a reality. And they are not the same" (Schneir, 2008). Shimba, 2010 explained that this means the reality of security is tied to the probability of different risks and how effective the strategies to mitigate the perceived risks are. It is also a feeling in the sense that; it is based on the psychological reactions to both the risks and the countermeasures (Shimba, 2010). Although no security breaches have been reported, but the instances of cloud outages resulting in loss of service to customers increases the reluctance and fuels the fear of adopting cloud computing. So Cloud computing needs to appeal to both the feelings of the potential customers and address the reality of the risks associated with cloud computing in a way that customers will feel safe and secure to use cloud computing.

On the challenges of trust, the user has to trust the services provider. That is, he has to trust the vendor on who it claims to be. In order to build trust in cloud computing adoption, there is a need to address the different situations or instances where trust is needed. Some of the instances where trust are needed are in order words, clients must trust cloud service providers as to the protection of their data, privacy and security of the use of the technology.

2.2 EXISTING SECURITY THREATS

Within a cloud environment we define as secure policy issues like "privacy, security, anonymity, telecommunications capacity, government surveillance, reliability and liability" [Sabahi, 2011]. There is a difference between each type of client a cloud server deals with. Academia clients require more performance than security protection in comparison with business clients that want their data to be protected more than having use on a high performance system. Gartner's seven security concerns will be described below.

- Privileged user access: Fragile data that can be analyzed from outsiders and give them the ability of bypassing the 'physical-logical' layer of the cloud and gain access on data and software.
- Regulatory compliance: Clients are responsible for the good management and security of their data, even in a cloud environment. Most cases show that percentage of data loss or privacy intrusion is caused from human factors that were clients.
- Data segregation: Encryption and decryption of data in the cloud is essential but it cannot be the only way of solution as it is vulnerable to attacks.
- Recovery: In case of server failure or denial of service how will the data of clients be restored? Does the cloud vendor have a backup plan of reverse engineer and protection of data? Are cloud managers capable of restoring data or they have to be supported from a third party company?
- Investigate support: Cloud services are hard to investigate because of many customers data placed in the same location, but can also spread infected files to other sets of software

Security issues posed by cloud computing

1. Distributed denial of service attacks
2. Employee negligence
3. Data loss and inadequate backups
4. Phishing and social engineering attacks
5. System vulnerabilities

III. Cloud Security Algorithms

The Data Encryption Standard (DES)

This is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). Figure 1 depicts the General Structure of DES in the following illustration

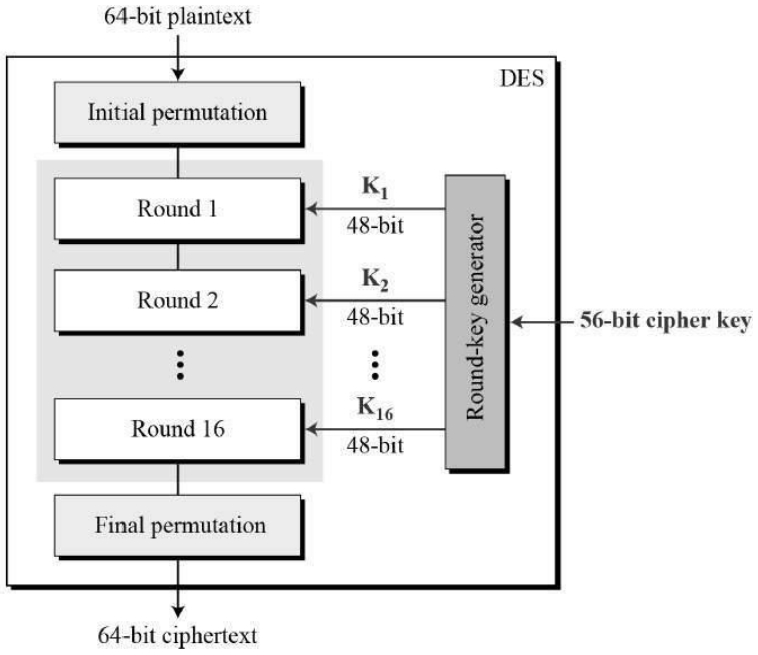

Figure 1: General structure of DES

Strength- The strength of DES lies on two facts:
a. The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.

b. The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

Weakness- Weakness has been found in the design of the cipher:
a. Two chosen input to an S-box can create the same output.
b. The purpose of initial and final permutation is not clear.

AES

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

Figure 2 depicts the schematic of AES structure

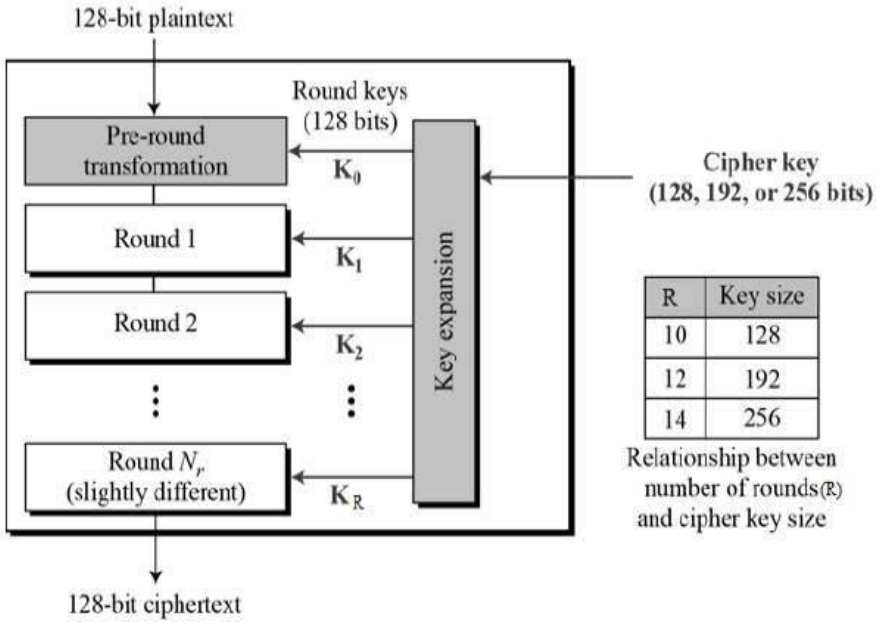

Figure 2 : Schematic of AES structure

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted in figure 3

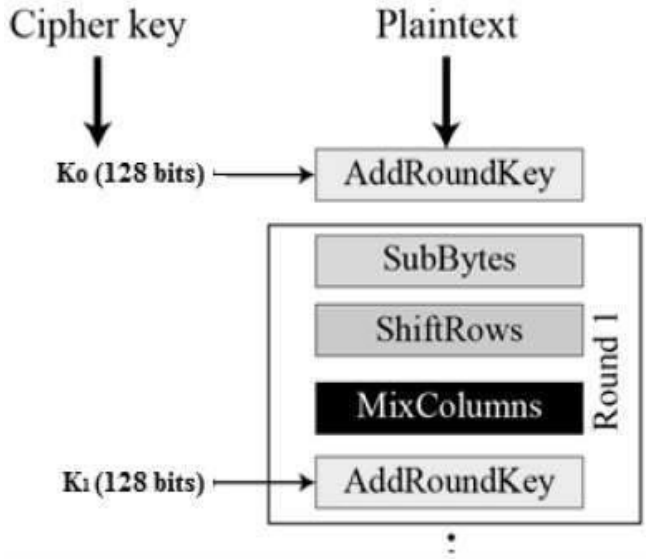

FIGURE 3: Encryption process

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four ro`ws and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

Benefits or advantages of AES

Following are the benefits or **advantages of AES**:

➡ As it is implemented in both hardware and software, it is most robust security protocol.

➡ It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.

➡ It is most common security protocol used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.

➡ It is one of the most spread commercial and open source solutions used all over the world.

➡ No one can hack your personal information.

➡ For 128 bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

Drawbacks or disadvantages of AES

Following are the disadvantages of AES:

➡ It uses too simple algebraic structure.

➡ Every block is always encrypted in the same way.

➡ Hard to implement with software.

➡ AES in counter mode is complex to implement in software taking both performance and security into considerations.

TDES

The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows in Figure 4

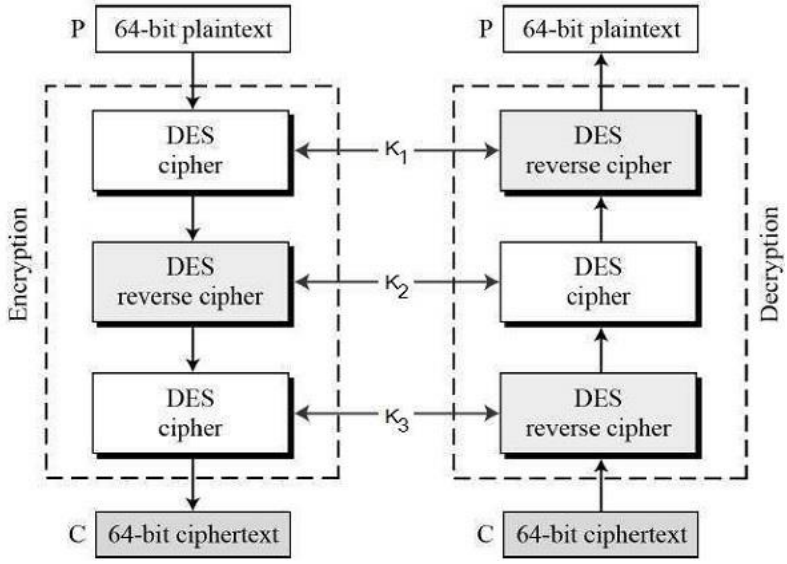

Figure 4: The encryption process

The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

3.2.4 Blowfish Algorithm

This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption

Advantages:

Blowfish algorithm is one of the fastest block ciphers in the general use, except when the changing keys. Each the new key requires pre-processing equivalent to the encrypting about 4 kilobytes of the text, which is very slow as compared to the other block ciphers. Blowfish algorithm is not the subject to any patents and is therefore freely available for anyone to use. This has contributed to its popularity in the cryptographic software.

Disadvantages:

The disadvantages of Blowfish algorithm are it must get key to the person out of the band specifically not through the unsecured transmission channel. Each pair of users' needs a unique, so as number of the user's increase, key management becomes complicated. Blowfish algorithm can't

provide authentication as well as non-repudiation as two people have the same key. It also has the weakness in decryption process over the other algorithms in terms of time consumption and serially in throughput.

3.2.5 RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Advantages of RSA Algorithm There are advantages and disadvantages of RSA algorithm. The advantages include; RSA algorithm is safe and secure for its users through the use of complex mathematics. RSA algorithm is hard to crack since it involves factorization of prime numbers which are difficult to factorize. Moreover, RSA algorithm uses the public key to encrypt data and the key is known to everyone, therefore, it is easy to share the public key.

The disadvantages include: RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer. It requires a third party to verify the reliability of public keys. Data transferred through RSA algorithm could be compromised through middlemen who might temper with the public key system. In conclusion, both the symmetric encryption technique and the asymmetric encryption technique are important in encryption of sensitive data.

Diffie-Hellman: is a key exchange algorithm and allows two parties to establish, over an insecure communications channel, a shared secret key that only the two parties know, even without having shared anything beforehand.

The shared key is an asymmetric key, but, like all asymmetric key systems, it is inherently slow and impractical for bulk encryption. The key is used instead to securely exchange a symmetric key, such as AES (Advanced Encryption Standard) used to encrypt subsequent communications. Unlike Diffie-Hellman, the RSA algorithm can be used for signing digital signatures as well as symmetric key exchange, but it does require the exchange of a public key beforehand.

RSA and Diffie-Hellman are both based on supposedly intractable problems, the difficulty of factoring large numbers and exponentiation and modular arithmetic respectively, and with key lengths of 1,024 bits, give comparable levels of security. Both have been subjected to scrutiny by mathematicians and cryptographers, but given correct implementation, neither is significantly less secure than the other.

The nature of the Diffie-Hellman key exchange does make it susceptible to man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange. This is why Diffie-Hellman is used in combination with an additional authentication method, generally digital signatures. When using RSA, a 1,024-bit key is considered suitable both for generating digital signatures and for key exchange when used with bulk encryption, while a 2048-bit key is recommended when a digital signature must be kept secure for an extended period of time, such as a certificate authority's key.

Getting back to the question at hand, you can't really merge the two algorithms because of the unique attributes and complexity that each one has. Most encryption systems offer a choice between them rather than combining them. SSL 3.0 supports a choice of key exchange algorithms, including the RSA key exchange when certificates are used, and Diffie-Hellman key exchange for exchanging keys without certificates and without prior communication between client and server.

IV. OBSERVATION

To assess the actual performance, we analyzed the performance of our algorithm by measuring the computation time of the encoding and decoding process for a data file, depending on the size (51 KB to 347,778 KB) and a variability of threshold (m,n); $1 \leq m \leq n$ and $n \leq 256$. We carry out these experiments on a Windows 7 Operating System (Redmond, WA, USA) with 8-core Intel Xeon E5-1620 (Santa Clara, CA, USA) at 3.50 GHZ with 32 GB of memory. In Figure 1, we have shown the computation time of the encoding operation. The encoding time for our algorithm mainly depends on the size of the data and the value of the (m,n) threshold. We obtained the computation time by summing the encryption time of x KB data plus the time to execute IDA with C-RS, and the time to hash and concatenate each slices file. The maximum encoding time is 14.15 s for a large data file equal to 347,778 KB with (200,254) threshold. We observed for different (m,n) configurations and data less than 347,778 KB that our encoding algorithm yields the best performance, since the average encoding time is 1.966 s.

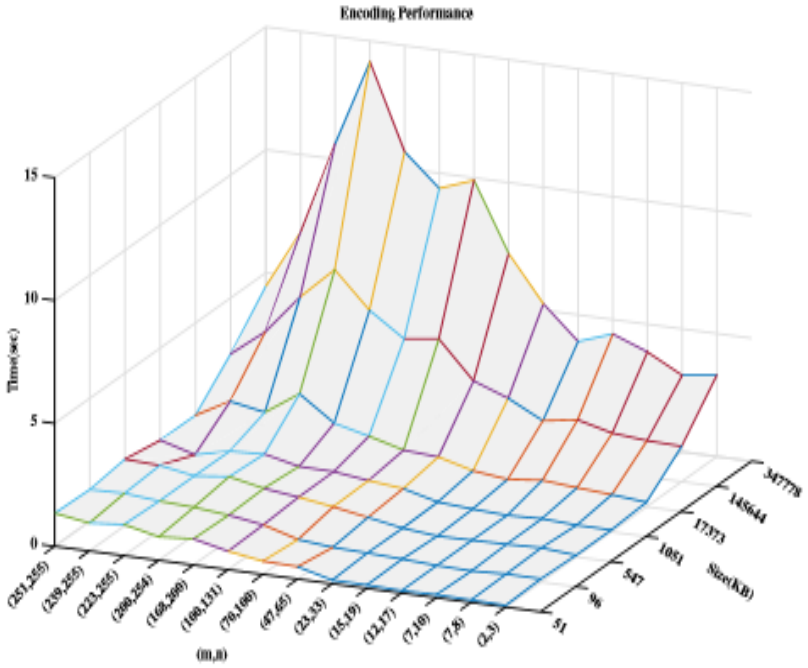

Figure 5: Encoding results

In Figure 3.5, the running time of the decoding operation has been shown. As we have described in Section1, the decoding time for x KB data file is equal to the sum of the different steps followed during the process. The maximum computation time is 24.30 s for 347,778 KB file with (2,3) and the average decoding time in this experiment is 2.907 s. The decoding process provides the highest performance for small and medium data size. However, the time required to decode x KB data depends primarily on the inner verification time and secondly on the reconstruction time. For large data size, these two processes become a bit computationally costly, but better than the preceding works. Depending on the value of (m,n), when the threshold is small, the verification time increases and the reconstruction time decreases. In addition, when the threshold is large enough, the verification time decreases dramatically and the reconstruction time increases. This will considerably reduce the decoding computation time. InTable1below, we displayed the average execution time for each inner step in the encoding and decoding processes.

Table 1. Average encoding/decoding time

Process	Duration
Encryption	0.367
Slicing-IDA	1.125
Hashing and concatenation	0.474
Verification	1.453
Reconstruction-IDA	1.157
Decryption	0.297

It is quite obvious that the encoding time is principally estimated by the slicing execution time, since it requires more parameters and computations than the other inner processes. Process Duration Encryption 0.367 Slicing-IDA 1.125 Hashing and Concatenation 0.474 Verification 1.453 Reconstruction-IDA 1.157 Decryption 0.297.

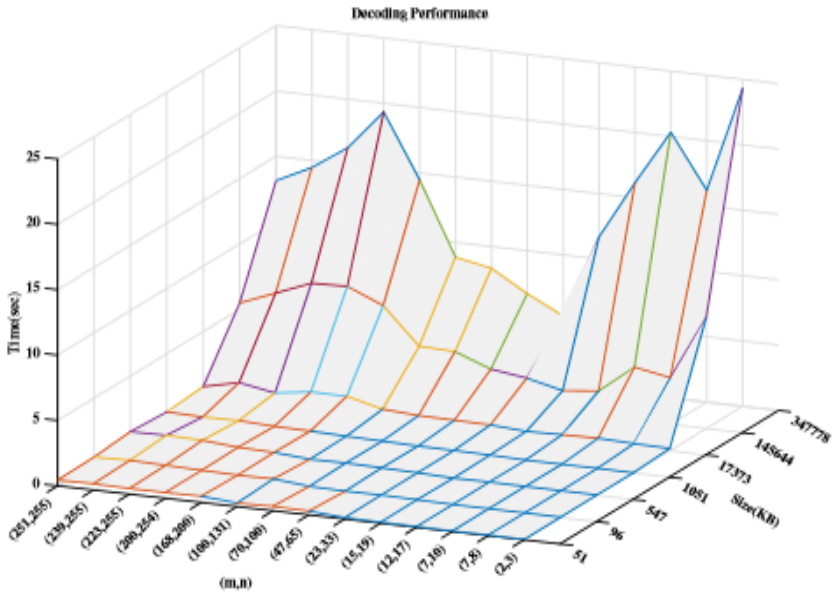

Figure 6 Decoding results

Encryption is everywhere; most of the products gathered today support a crypto graphic algorithm and particularly AES. Even those that support other algorithms tend to recommend using AES. However, most of the cryptographic algorithms (AES, RSA, etc.) are not secure against quantum computing. Some products that encrypt files, not at whole-disk solutions like VeraCrypt. Boxcrypor: is a file-encryption software designed and created specifically for cloud use, with support for all major cloud-storage providers. The user has the ability to encrypt, decrypt, share, add and remove files from cloud storage directly through his/her end device. Furthermore, there is a possibility to protect files by encrypting them locally before posting to a cloud-storage provider, ensuring file security and file-data privacy throughout the process.

Boxcryptor

Uses AES-256 and RSA encryption algorithms. It ensures data accessibility, confidentiality and privacy protection. SecureDoc CloudSync: designed by WinMagic, is an enterprise endpoint encryption solution that encrypts data at rest on endpoint devices before they are stored in cloud, providing an added layer of security to that offered by the storage service provider.

SecureDoc CloudSync

Uses Advanced Encryption Standard–New Instructions (AES-NI) 256-bit encryption. It provides data confidentiality and data privacy but does not prevent eavesdropping. In regard to these two product solutions and their development, it is quite obvious that they provide faster execution time than the proposed methodology since both are relying upon encryption, which corresponds to the first layer of our algorithm (AES-256). However, their use ensures data confidentiality and privacy but does not guaranty data integrity and availability. However, our implementation enhances data CIA (Confidentiality-Integrity-Availability). Confidentiality is achieved by combining AES-256 and IDA, integrity by concatenating each particular slice file with its corresponding SHA-512 hashcode, and, finally, data availability is accomplished by dispersing (IDA) the resulting data slices, as we suggested earlier in Section.

V. CONCLUSION

This paper included all the latest security tools and models for cloud environments and a review was given for each of them and system requirements and cloud management where investigated. Every system has goals and requirements. In order to maintain a complex system like a cloud, management teams have to be set up and have assessed privileges.

REFERENCES

[1]. Ahmadi, M. and Moghaddam, F.F.; Jam, A.J.; Gholizadeh, S.; Eslami, M. A 3-level re-encryption model to ensure data protection in cloud computing environments. In Proceedings of the IEEE Conference on System, Process & Control , Kuala Lumpur, Malaysia, 12–14 December 2014.

[2]. Alexa H. and James C. 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. (2011).

[3]. Anitha Y, "Security Issues in cloud computing", "International Journal of Thesis Projects and Dissertations "(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.

[4]. Arockiam, L. and Monikandan, S. Efficient cloud storage confidentiality to ensure data security. In Proceedings of the International Conference on Computer Communication and Informatics, Coimbatore, India, 3–5 January 2014; pp. 1–5.

[5]. Balamurugan, S.; Sathyanarayana, S. and Manikandasaran, S.S. ESSAO: Enhanced security service algorithm using data obfuscation technique to protect data in public cloud storage. Indian J. Sci. Technol. 2016.

[6]. Cloud Computing. Available online: https://en.wikipedia.org/wiki/Cloud_computing#Security_and_ privacy (accessed on 8 February 2017).

[7]. Abdul D. S. and Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
[8]. Gurpreet S. and Supriya K. "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
[9]. Garima S. and Gurgaon N. S., "Triple Security of Data in Cloud Computing". Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (4).2014,
[10]. Jaeger, B. Security as a Service Working Group, Defined Categories of Security as a Service (Preview)—Continuous Monitoring as a Service. Cloud Security Alliance 2016. Available online: https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categoriessecurities-prep.pdf (accessed on 10 August 2016).
[11]. Li, M. On the Confidentiality of Information Dispersal Algorithms and Their Erasure Codes. arXiv 2013, arXiv:1206.4123v2.
[12]. Mar, K. K.; Law, C. Y. and Chin, V. Secure personal cloud storage. InProceedingsofthe10thInternationalConference for Internet Technology and Secured Transactions (ICITST-2015), London, UK,14–16December2015.
[13]. Mask Sensitive Data. Available online: https://dataapps.io/redact.html (accessed on 12 January 2017).
[14]. Minowa, T. and Takahashi, T. Secure Distributed Storage for Bulk Data; Springer: Berlin/Heidelberg, Germany, 2012; pp. 566–575.
[15]. Mishra, B. and Jena, D. Securing files in the cloud. In Proceedings of the 2016 IEEE International Conference on Cloud Computing in Emerging Markets, Bangalore, India, 19–21 October 2016.
[16]. Gurjeevan S., Ashwani S and Sandha S. K. "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.
[17]. NIST, Cloud Computing Program–29 July 2016: Cloud Computing. Available online: https://www.nist. Gov/ programs-projects/cloud-computing (accessed on 13 January 2017).
[18]. Press Releases. Cloud Storage Security Challenges. Available online: https://www.nasuni.com/news/26top_5_security_challenges_of_cloud_storage/ (accessed on 5 April 2017).
[19]. Qi. Zhang ·Lu. Cheng, Raouf Boutaba, "Cloud computing: state-Of-the-art and research Challenges", "The Brazilian Computer Society", April 2010.
[20]. Rabin, M.O. Efficient dispersal of information for security, load balancing, and fault tolerance. J. ACM 1989, 36, 335–348.
[21]. Raj, G.; Kesireddi, R.C.; Gupta, S. Enhancement of security mechanism for confidential data using aes-128, 192 and 256 bit encryption in cloud. In Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies, Dehradun, India, 4–5 September 2015.
[22]. Rancourt, C. Celebrities Hacked: Are Your Personal Photos Safe in the Cloud? Available online: http:// www.nextadvisor.com/blog/2014/09/02/celebrities-hacked-personal-photos-cloud-safe/ (accessed on 13 January 2017).
[23]. Rich, S.; Gellman, B. NSA Seeks to Build Quantum Computer That Could Crack Most Types of Encryption. Available online: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-buildquantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8defa33011492df2_story.html?utm_term=.217ad6b56479 (accessed on 14 July 2016).
[24]. Ruben king, N. J. The Best Encryption Software of 2017. Available online: http://www.pcmag.com/article/347066/the-best-encryption-software-of-2016 (accessed on 5 June 2017).
[25]. Sarada, G.; Abitha, N.; Manikandan, G. and Sairam, N. A few new approaches for data masking. In Proceedings of the 2015 International Conference on Circuit, Power and Computing Technologies, Nagercoil, India, 19–20 March 2015.
[26]. Singh, S.; Kumar, V. Secure end user's authentication and private data storage access scheme in cloud computing using elliptic curve cryptography. In Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development, New Delhi, India, 11–13 March 2015.
[27]. Smith, C. Point The Year of BYOE (Bring Your Own Encryption). Available online: https://cipherpoint.com/ 2014/06/2014-the-year-of-byoe-bring-your-own-encryption/ (accessed on 15 June 2016). Finite Field. Available online: https://en.wikipedia.org/wiki/Finite_field (accessed on 8 February 2017).
[28]. Stallings, W. Cryptography and Network Security Principles and Practices, 6th ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2005.
[29]. Surv, N.; Wanve, B.; Kamble, R.; Patil, S. and Katti, J. Framework for client side aes encryption technique in cloud computing. In Proceedings of the IEEE International Advance Computing Conference, Bangalore, India, 12–13 June 2015; pp. 525–528.
[30]. Suthar, K. and Patel, J. Encry Scation: A novel framework for cloud iaas, daas security using encryption and obfuscation techniques. In Proceedings of the 2015 5th Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, 26–28 November 2015.
[31]. Uma S., "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,"2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).
[32]. Wall, M. Can We Trust Cloud Providers to Keep Our Data Safe? Available online: http://www.bbc.com/ news/business-36151754 (accessed on 29 April 2016).
[33]. White Paper. Securing Sensitive Data within Amazon Web Services Ec2 and Ebs: Challenges and the Solutions to Protecting Data within the AWS Cloud. Copyright 2013 Vormetric. Available online: http://go.thalesesecurity.com/rs/480-LWA-970/images/wp-securing-data-within-AWS. Pdf (accessedon 29 April 2016).
[34]. Wolfgang, G. Cost Reduction Remains Chief Reason to Adopt Cloud, Confusion Still Apparent. Available online: http://www.tomsitpro.com/articles/cloud_survey-kpmg-tech_adoption-provider-it_security,1803.html (accessed on 7 January 2017).
[35]. Yogesh K., Rajiv M. and Harsh S., "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.
[36]. Zhang, X. and Wang, H. A study of the use of idas in cloud storage. Int. J. Future Comput. Commun. 2013, 2, 67.

AUTHOR'S BIOGRAPHIES

Dr. O. I. Omotosho is a Senior Lecturer at the Department of Computer Science and Engineering, Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria, where she teaches undergraduate and postgraduate students, supervises students' project/thesis and does research in the area of Web Informatics/Information Systems, Data Analytics/Management and Software Engineering. She has several peer reviewed journal and articles conference papers.

