Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(6):59-66**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

A Cloud-Based Data Security System using Advanced Encryption (AES) and Blowfish algorithms

UGBA T. PIUS[1], EZE C. ONYEBUCHI[2], OGIDI P. CHINASA[3], EKLE F. ADOBA[4]

[1]Department of Computer Science and Statistics, Akperan Orshi College of Agriculture, Yandev, Benue State, Nigeria
[2]School of Education, Federal College of Education, Eha-Amufu, Enugu State, Nigeria
[3]Department of Computer Science Technology, Federal College of Agriculture, Ishiagu, Ebonyi State, Nigeria
[4]Senior Program Analyst, Planning Research and Statistics Unit, Federal Medical Centre, Makurdi

Abstract This paper develops a cloud-based data security using advanced encryption standard (AES) and blowfish algorithms to enhance information security in cloud computing. Cloud computing is a technology that offers hosted services over the Internet. It provides a distributed computing environment through which people can share resources, services and information among themselves through the use of internet. However, due to the high growth in the field of cloud computing, data privacy, data confidentiality, data security and data integrity became the major threats to the full adoption of this promising technology. These security challenges pose serious danger to cloud computing and need to be enhanced and resolved. The researcher proposed a new security system for cloud computing which introduces a mechanism through which information can be protected from unauthorized users. In this system, a combination of Advanced Encryption Standard (AES), Blow Fish algorithm and Short Message Service (SMS) are implemented to enhance data security in the cloud. Their combined features provide three way security: confidentiality, authentication and verification. AES encryption algorithm is proposed for confidentiality of data, Blow Fish algorithm for authentication and SMS for verification. The new security system addresses issues of privacy, confidentiality, security and integrity of data stored in the cloud. The resulting application is designed using Object Oriented Analysis and Design Method (OOADM) and is implemented using C# programming language and MYSQL database.

Keywords Cloud computing, AES, Blowfish, information security

Introduction

Cloud computing is a new archetype that can provide self-service on demand and at a minimal cost. It is gaining popularity in all spheres including schools, government and non-governmental organizations. One of its advantages 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.

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.

Review of Related Literature

For the fact that we are already into the 21st century, no organization, company or institution of higher learning can do without cloud computing. Many authors and researchers have in one way or the other taken steps towards analyzing cloud computing technology and the numerous unresolved security issues threatening the cloud computing adoption.

In [1] a design was proposed 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 [2] 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 [3] 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.

[4] 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.

[5] 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.

[6] 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.

Cloud Security Issues

Security is a big challenge in cloud systems due to its nature of outsourced computing [7]. 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 [8].

According to [7], 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 [7]. 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 [7]. 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.[9] provided security topics in terms of cloud computing based on analysis of Cloud Security treats and technical components of Cloud Computing. He listed some threats for cloud service users as:

i. **Responsibility Ambiguity:** Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility

among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).

ii. **Loss of Trust:** It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the provider's security level in formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the provider. Such a lack of sharing security level in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.

iii. **Unsecure Cloud Service User Access :** As most of the resource deliveries are through remote connection, non-protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

iv. **Data loss and leakage:** The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside. For example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability; and disaster recovery can be recognized as major behaviours in this threat category.

Methodology

The researcher proposed a new security model that provides a mechanism through which communication can get 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 block diagram of the proposed security model is depicted in Figure 1.

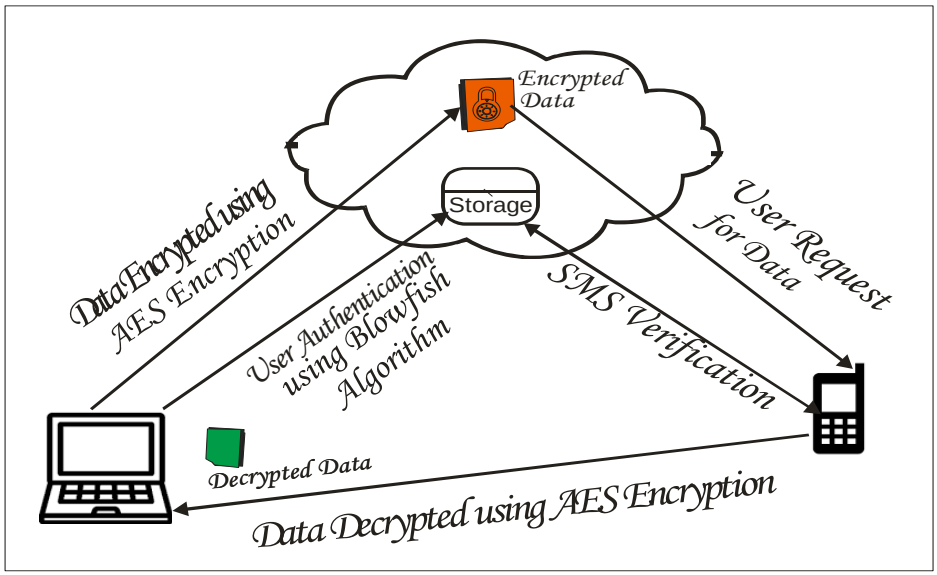

Figure 1: Proposed security model

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.

Advanced Encryption Standard (AES)

In November 26, 2001 the Federal Information Processing Standards Publication 197 announced Advanced Encryption Standard (AES) as a standardized form of the Rijndael algorithm as the new standard for encryption [10]. 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 [11]. 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 [12]. 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 AddRoundKey stage. However, before reaching the final round, this output goes though 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 [13]. 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 according to [14].

i. 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 Rijndael Sbox.
ii. 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.
iii. 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.
iv. 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.

Blowfish Algorithm

Bruce Schneier designed blowfish in 1993 as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm [15] 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 [15].

Basically, Blowfish encryption algorithm requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles [16] 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. 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 ciphertext. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.

Results

Implementation of our 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 Silverlight.
The developed application produces physical results. These results are the outcome or output of the application which are in accordance with the requirement of the system. The outcome or output of the application are presented below with each output carrying its title that explains what it does in the developed system.
Figure 2 shows the login screen of the developed security framework. The page enables registered users to login and upload data to cloud. If the username and password entered by the user are valid, the software will open the main page where the user will securely upload and download files. On the other hand, if a user enters an invalid password, a message will be sent to the owner of the account informing him of someone trying to gain access to his account.

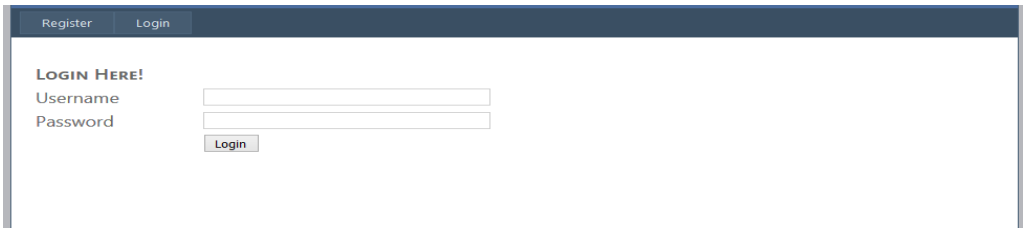

Figure 2: Login Screen

If a user is successfully authenticated, he is redirected to Figure 3 (file upload page) where he can upload and download data. In the upload files section, a user 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.

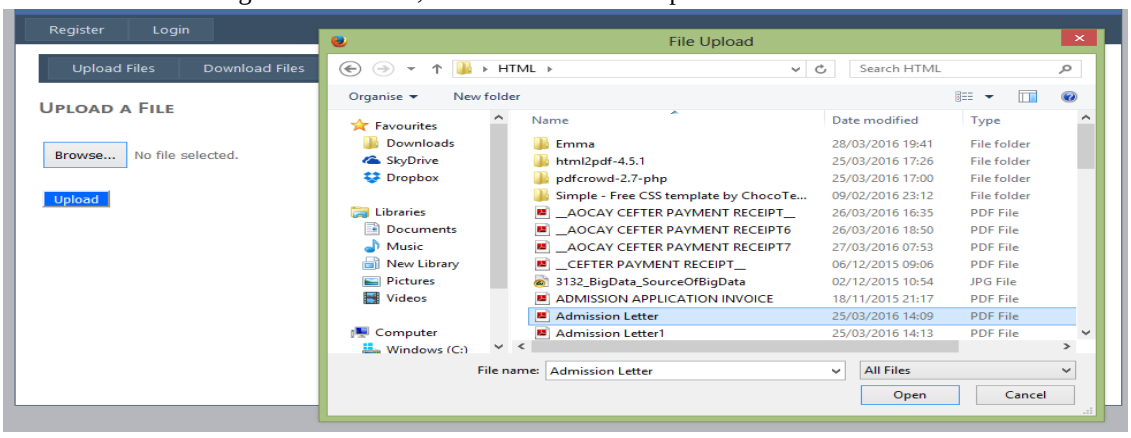

Figure 3: File Upload Page

Figure 4 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.

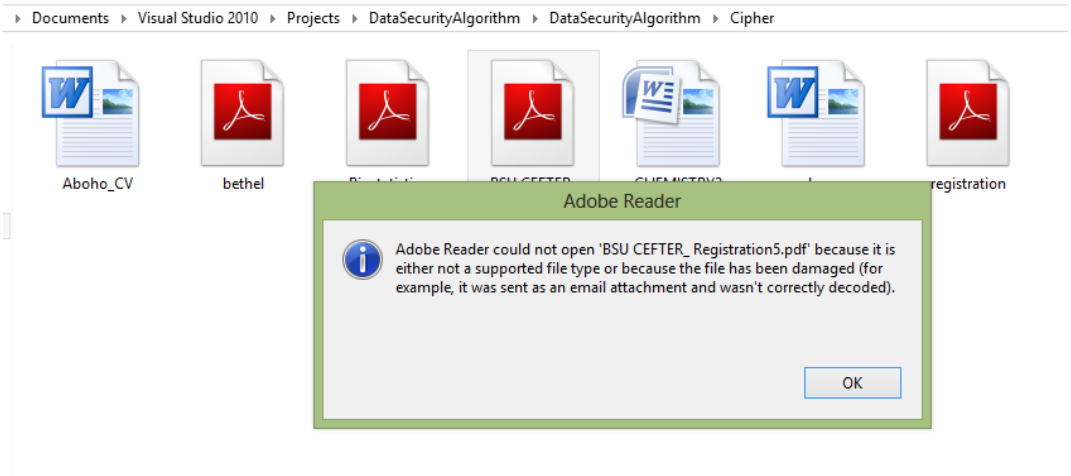

Figure 4: Encrypted Files

Conclusion

In this paper, the problem of data security in cloud computing, which is essentially a distributed storage system was analyzed. To provide data confidentiality and information integrity of users' data in cloud computing environment, we proposed an effective security model that provides a mechanism through which communication can be protected as well as hides the information from unauthorized access. Our security model allows the cloud users to securely handle the privacy and integrity of their data stored in the cloud without relying on the credibility of the cloud provider. The application of AES algorithm, Blowfish encryption and SMS verification in cloud computing would provide a strong base which protect data stored in cloud as well as enable access to data only on successful authentication and verification. The security model can be enhanced in the future to encrypt video and audio files but not just text files.

References

[1]. Suganya S. and Damodharan P. "Enhancing Security for Storage Services in Cloud Computing." International Journal of Scientific and Research Publications, 3(6), pp1-3 (2013).

[2]. Sumita, L. and AjayK. "An Approach for Ensuring Security in Cloud Environment." *International Journal of Advances in Computer Science and Technology*, 3(2), pp 92-95. (2014).

[3]. Deepika V. and Karan M. "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. (2014).

[4]. Manoj K. and Kranti A. "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 (2014).

[5]. Sudhansu R. L. and Biswaranjan N. "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(2014).

[6]. Ranjit K. and Raminder, P. S. "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques." *International Journal of Mobile Computing & Application,* 2(3), pp 38-44. (2015).

[7]. Jens-Matthias B., Nils G., Meiko J., Luigi L., and Ninja M., "Security and Privacy Enhancing Multicloud Architectures". IEEE Transactions on Dependable and Secure Computing, 10(4), pp212-224. (2013)

[8]. Arijit U., Debasish J., and Ajanta D. "A Security Framework in Cloud Computing Infrastructure". International Journal of Network Security & Its Applications, 5(5), pp 11-24 (2013).
[9]. Kangchan L., "Security Threats in Cloud Computing Environments." International Journal of Security and Its Applications 6(4), pp 25-32. (2012).
[10]. Douglas, S. "Advanced Encryption Standard." Rivier Academic Journal, 6(2), pp1-14, (2010).
[11]. Deep Kaur, P., and Inderveer, C., "Unfolding the Distributed Computing Paradigm," *International Conference on Advances in Computer Engineering (ACE 2010)*, June 21-22, 2010, Bangalore, India. (2010).
[12]. Gurjeevan, S., Ashwani, S. and Sandha, K. S. "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System," *International Journal of Multi-disciplinary Research*, 1(4), pp. 143-151. (2011).
[13]. Zilhaz, J. C., Davar, P. and Nishantha, G. G. D. "AES and Confidentiality from the Inside Out," *the 12th International Conference on Advanced Communication Technology (ICACT)*, pp. 1587-1591. (2010).
[14]. Akash, K. M., Chandra, P. and Archana, T, "Performance Evaluation of Cryptographic Algorithms: DES and AES", *IEEE Students' Conference on Electrical, Electronics and Computer Science*, pp. 1-5. (2012).
[15]. Pia, S. and Karamjeet, S. "Image Encryption and Decryption using Blowfish Algorithm in Matlab." *International Journal of Scientific & Engineering Research*, 4(7), pp 150-154 (2013).
[16]. Saikumar, M. and Vasanth, K. "Blowfish Encryption Algorithm for Information Security." *ARPN Journal of Engineering and Applied Sciences*, 10(10), 4717-4719 (2015).