An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography

Adamu Ismail Abdulkarim, Boukari Souley

Abstract—cloud computing is a collection of configurable shareable resources accessible via the internet. Cloud computing save individuals and organizations the cost of buying and maintaining resources such as memory storage, software, network, server, operating system by using the one available on cloud by paying according the resources used. The major drawback of cloud computing is security challenges. This is because cloud resources are managed by third party. Some security techniques such as cryptography and steganography are used to protect data to be stored on the cloud from intruders. This work proposed an enhanced security system using RSA as digital signature and image steganography to improve the security of data stored on the cloud in order to prevent the access of those data when uploading or downloading them from the cloud from unauthorized users and also evaluate the efficiency of the system by measuring the computing resources such as memory storage, CPU processing, power and network bandwidth consumed by the algorithms using different data types and size.

Index Terms— Cloud computing, Cryptography, Steganography, RSA, DSA, Cloud security.

1 INTRODUCTION

Cloud computing is an emerging technology in the field of information technology (IT). It is an infrastructure that provides accesses to various resources such as server, network, operating system and storage space for use by user payable on demand [34, 31]. Cloud computing allows organizations and individuals to make use of the resources available on the cloud to save them the cost of buying and maintaining the resource themselves [35]. There are several kinds of cloud computing deployment models like Private cloud, Public cloud, Community cloud and Hybrid cloud [39]. The infrastructure of cloud computing is made up of some underlying service models such as software as a service model (SaaS), Platform as a services model (PaaS) and infrastructure as a service (IaaS) [23]. The resources used in cloud computing are managed by third party, this becomes a serious concern to the user because the user may not know who is accessing their data in the cloud and whether changes are made on the data since the third party has full control on the data once it is sent to the cloud [25].

There are two types of threat attacks in cloud computing [2]. The first threat is the internal threat which is a major threat from the cloud service provider administrator whom might make some illegal accesses to user data or even make changes to the data without the user consent since the user does not have control over his data in the cloud. The second threat is the external threat. This kind of threat is majorly from hackers/intruders whom might gain illegal access to the resource in the cloud without paying for it or have illegal access to user data in the cloud and even damage the data or make changes on them. However, as the demand access to cloud resources increases on daily basis the need to protect those resources from unauthorized users becomes paramount in order to avoid interference and modification of resource by malicious users [13].

The security of data in cloud includes confidentiality which ensures that the data is only accessible by the intended user, integrity which ensures that the content of the data is not changed from its original form when accessed by the user and availability which ensures that the data is available to the user anytime, anywhere on the cloud [20].

Many techniques have been adopted by researchers to secure their data in the cloud among such techniques are cryptography and steganography [29]. Cryptography is the science of converting plaintext into cipher text, a form that is not understood by an unauthorized user [3]. Cryptographic algorithms such as symmetric and asymmetric algorithms are used in the cloud environment to secure data and application from malicious users and unintended third party to prevent data theft and unauthorized access [30]. Steganography is the art and science of hiding data such that it existence is concealed from unauthorized users [6]. The science of steganography involves hiding message such as video, audio, text and image file within another such that it appear innocent and not draw attention of intruders [17]. Steganography can be classified into image, video, text and audio steganography [27].

However, this work is aimed at providing security on data to be uploaded or downloaded from the cloud using RSA as digital signature and image steganography and also to evaluate the performance of the algorithms using different data types and size in order measure the computing resource such as memory storage, CPU processing, power and network bandwidth consumed by the algorithm. The advantage of combining cryptography and Steganography is that, if the intruder tries to decrypt the encrypted data, the content will be concealed from him because steganography will make the content look innocent and meaningless to the intruders. In the other hand if the intruders is able to suspect that there is steganography in the content and he extract it,

- Adamu Ismail Abdulkarim is currently pursuing his Master Degree in Computer science, Department of mathematical science, Abubakar Tafawa Balewa University (ATBU), Bauchi, Nigeria. Email: psalmlisticforlife@yahoo.com
- Boukari Souley Department of Mathematical Sciences, Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria. Email: **bsouley2001@yahoo.com**

decrypting the data will be difficult for him using Encryption Algorithm.

The remaining part of this work is summarized as follows: Section2 discussed related works. Cloud security challenges are discussed in Section3. In Section4 security techniques used in cloud computing such as cryptography and steganography were presented. Methodology, proposed work and architecture of the system is presented in Section5. Section6 present the simulation tool to be used for the system implementation. Section7 discussed the conclusion and future work.

2 RELATED WORK

This section gives a review of work done by researchers on cloud security. In [20] the authors performed analysis on various symmetric and asymmetric cryptographic algorithms used in cloud. The research analyzed the strength of the key length and security of Data Encryption Standard (DES), Advance Encryption Standard (AES), Triple Data Encryption Standard (TDES), Blowfish, International Data Encryption Algorithm (IDEA), Rivest Shamir Adleman (RSA) and Hormomophic Algorithms. In the study it was concluded that the algorithms analyzed are not strong enough, it can easily be broken by intruders. They suggested that a stronger security majors need to be developed that will guarantee the security of user data in the cloud. In [32] the authors evaluates Data Encryption Standard, Advance Encryption standard and Blowfish symmetric encryption algorithms considering the speedup of the algorithms that is the time it takes for the algorithms to start and finish encryption, the mean time that is the difference between the algorithms execution time in the cloud and on the system, and the buffer size consumed by the algorithms using data size of 10, 13, 39 and 56kb. In [4] the authors evaluate some symmetric, asymmetric and hashing cryptographic algorithms. The research considered Encryption and Decryption time, CPU processing power and size per payload to be used in the cloud as metrics. In their research, it was concluded that AES has good key encryption capability and MD5 to be the fastest in terms of data encoding. The authors in [28] proposed security of cloud data using AES algorithms with 10 rounds and 128 keys. The research performs comparison of Advance Encryption Standard (AES) with some other algorithms like Data Encryption Standard (DES), Triple Data Encryption standard (TDES) and Rivest Cipher2 (RC2). The study in [13] proposed a security based system on RSA cryptographic algorithms using space complexity, time complexity and throughput to measure the performance of the algorithms. The authors in [19] evaluated the performance of some selected symmetric and asymmetric algorithms used to encrypt data in cloud environment and the changes that occurs in the size of the data after it has been encrypted. The research uses only text and document data to evaluate the performance of the algorithms when several other data like video, audio, image can also be used. In [26] *a* comparison analysis of some selected symmetric and asymmetric encryption algorithms such as DES, 3DES, Blowfish, AES, IDEA, RSA using the speed, block size, security strength and key length of the algorithms as a performance measure to evaluate the algorithms was critically carried out. The authors in [24] proposed a security algorithm in cloud to eliminate problem attached to data loss, segregation and security when accessing data in the cloud. The research conducts a comparative analysis on some selected symmetric encryption algorithms such as DES, 3DES, Blowfish and AES to ensure data security in cloud. In [30] the authors proposed a multilevel security on Document Management System (DMS) in cloud using Advance Encryption Standard (AES) and Riverst Shamir Adleman (RSA). The study focuses on providing security to document management system in cloud. The authors in [38] proposed the use of full Homomorphic encryption algorithms to secure data in the cloud environment. In the research, only the security capability provided by the algorithms was considered but the speed of the algorithm during data encryption and decryption and computing resources consumed by the algorithm was not put into recognition. The authors in [2] Improved classical encryption algorithm by integrating two algorithms Substitution Cipher and Transposition Cipher in order to prevent access to user data in cloud either by cloud administrator or by intruders. Their work provides security to cloud data by hybridizing substitution cipher and transposition cipher since user has no control on data once the data has been uploaded to the cloud service providers (CSP). The proposed algorithms make user data not accessible by both cloud service provider administrator and intruders once the data has been encrypted and uploaded to the cloud. The authors in [33] Provides security on cloud data using blowfish encryption algorithms. In their work, the Blowfish algorithm is used to secure cloud data from an unauthorized access. Any attempt to access secured data in the cloud a compare is invoked to verify the source of the access and an alert is send to notify the user that someone is trying to access his/her data. Their work provides security to cloud data using encryption and Simple Object Access Protocol (SOAP). In [7] the authors implemented triple encryption algorithms to provide security for cloud data. In their study, they used Digital Signature Algorithms (DSA), Advance Encryption Standard (AES) and Steganography to secure cloud data over a network. The DSA is used to authenticate between users in order to ensure that the data is accessed by a valid user, the AES is used to encrypt the data and make it unreadable by an un authorized user and the Steganography is used to hide the data within the audio files such that only the user will be able to use it. Their work provides strong security and privacy to cloud data but consumes more time when encrypting and decrypting the data because each of the algorithms has to be implemented one after other. The authors in [36] developed Hybrid algorithms using Riverst Shamir Adleman substitution (RSA), Mono- alphabetic substation and Ceaser cipher to provide privacy to data in cloud. The proposed Hybrid algorithm is used to validate access to data in the cloud. To login to the cloud the user private key (Username and password) is first encrypted with Ceaser cipher, the encrypted result is now also encrypted with RSA substitution algorithms and the final result is now encrypted again using the mono-alphabetic substation method. The proposed algorithm provides privacy to cloud data but consumes more processing time since the algorithms need to be implemented one after the other. The authors in [10] proposed a hybrid encryption algorithm using Rivest Shamir Adleman (RSA) as a digital signature and Blowfish for encryption. The RSA algorithm is used to provide a message digest to authenticate the user by generating public and private key. The public and private key is used for authentication and not repudiation. Once the data has been authenticated, it's then encrypted using blowfish.

3 CLOUD SECURITY CHALLENGES

Cloud computing has some major security issues and challenges stated in [22] as follows:

3.1 Data Issues

Data in cloud can be access at any time by any user once he/she have access to network. The privacy of sensitive data in the cloud becomes a very serious issue since any one can have access to the data. Some malicious user or even the cloud service providers might make changes to the data in cloud without the consent of the user since the user does not have control over the data once it is sent to the cloud. Also data stealing and data lost is another issue in cloud computing. Data can be stolen in the cloud when been transferred from the cloud. Due to the above challenge, integrity and viability of data need to be maintained by cloud service providers.

3.2 Secrecy Issue

Sensitive and delicate data are sent to the cloud and the security of such data is paramount to the service provider in order to prevent unauthorized access to those data by other providers and users. Since the servers are mostly external, the provider should be able to take necessary measures to validate who is accessing the data in the cloud and who is maintaining the cloud servers so as to prevent interference of user data by illegal users.

3.3 Infected Applications

In cloud computing several applications are developed and uploaded by individuals and organization. The cloud service providers need to take full responsibility of monitoring and maintaining the server so as to prevent malicious users from uploading corrupt or infected files to the cloud that could affect or damage order data already uploaded to the cloud by other developers.

3.4 Security Issues

Security and privacy of data in cloud is very important to cloud service providers since sensitive and delicate data are uploaded on daily basis to the cloud. The security of data in the cloud should be in two ways. Firstly, the user should provide security to his/her data either by encrypting it or by providing means of authentication by the use of digital signature before sending the data to the cloud. Secondly the cloud service provider should provide security to the data uploaded to the cloud by ensuring that only valid users gain access to the data in the cloud in order to prevent data stealing, damage or loss in the cloud.

4 Security Techniques Used In Cloud Computing

4.1 Cryptography

Cryptography is the art and science of hiding information or data from unintended users [14]. Some examples of symmetric and asymmetric cryptographic algorithms are discussed below:

4.1.1 Symmetric Encryption Algorithms

Symmetric key encryption algorithms also known as private key encryption used the same key for both encryption and decryption [1]. Some example of Symmetric key encryption algorithms are discussed below:

A. Data Encryption Standard (DES)

DES is a block cipher symmetric encryption algorithm with key size of 64 bit. It was the first encryption algorithm developed by IBM and accepted for use by America National Institute of Standard and Technology (NIST) in1977.DES algorithms used only 56bits of it is data for encryption and the remaining 8bits is used for error detection. DES is considered in-secured because of it small key size and was replaced by Triple Data Encryption Standard.

B. Triple Data Encryption Standard (3DES)

3DES it is an improvement of DES algorithms. 3DES uses 192 bit key size because it uses three times the 64 bit keys length used by DES to encrypt and decrypt data. The encryption process of 3DES is similar with that of its predecessor just that 3DES applied three times DES to increase the security level of the data and that makes it one of the slowest block symmetric ciphers used today.

C. Advance Encryption Standard (AES)

AES algorithms was developed in 1998 and accepted by National Institute of Science and Technology America (NIST) in 2001. The algorithm was considered a replacement for DES and 3DES because of it key strength and flexibility. Today AES is accepted and used worldwide. AES encrypts data block of 128bit, 192bit and 256bit in 10, 12 and 14 rounds respectively. AES is used on varieties of devices and applications because of its flexibility and key strength.

D. Blowfish

Blowfish is 64bit block cipher with variable key lengths ranging from 32 to 448. As stated in [16] Blowfish algorithm consists of two parts: key expansion part and data encryption part. Key expansion converts the key into several sub key arrays of total 4168 bytes. Data encryption part is done via 16 round Feistel network. Each round consists of the key permutation, and the key and data dependent substitution.

4.1.2 Asymmetric Encryption Algorithms

Asymmetric key encryption algorithms also known as public key encryption algorithms use different keys, private and public keys for encryption and decryption unlike the symmetric key encryption algorithms [11]. Examples of some asymmetric key encryption algorithms are discussed below:

A. Rivest Shamir Adleman (RSA)

RSA is asymmetric key encryption algorithm developed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman [10]. It was named after its developers Rivest, Shamir and Adleman. It uses two keys, public key and private key. The public key is known by all users while the private key is only known to the valid users for authentication and verification. The activities in RSA involve key generation, encryption and decryption. The key length of RSA ranges from 1042 to 4096.

B. Digital Signature Algorithm (DSA)

A digital signature algorithm is an electronic key used for verification and authentication of user or data in the cloud. The algorithm was initiated by National Institute of Science and Technology USA in 1991 to be used in their Digital signature standard (DSS) and was incorporated in 1993. The algorithm works by first of all making choice of encryption parameters which will be shared across several users of the system and then in the second stage private and public key is created for single user. The signature is created with the private key by the sender and then it's verified and authenticated by the receiver using the public key. DSA has a key size of 3072 bits.

However, cryptography has some challenges when handling complex data such as those in the cloud where the data are kept in different locations and processed from different data centers; the means of the transfer of these data from one location to another on the cloud would make the data appear suspicious to intruders because cryptography cannot hide the existence of these data during transfer from intruders [5].

4.2 Steganography

Steganography is the science of hiding the existence of communication or data transfer such that it remains secret from an unauthorized third party [9]. The word steganography is driven from a Greek word which means concealed writing. The word "Steganos" means "Covered" and "graphial" means "Writing". According to [8, 9, 27] Steganography can be described into the following types:

4.2.1 Text steganography

This technique involves hiding the existence of communication within a text file. In text steganography, the text used for communication is formatted by altering the arrangement of the text without affecting it real content in order to achieve a secure communication. The method involves line shift coding, word shift coding and feature coding.

4.2.2 Image steganography

Image steganography is the process of hiding the existence of data to achieve a secure communication by using image cover. In this technique, the content to be transferred is hidden within an image folder in order to make the content not to look suspicious to intruders. There are different methods used for image steganography such as least significant bit insertion, Masking and filtering, redundant pattern encoding, encrypt and scatter, and Algorithms and transformation.

4.2.3 Audio steganography

In audio steganography, secret messages are transferred using audio files of different format such as WAV, MP3 and AU. There are several methods used for audio steganography such as least bit encoding (LSB), Phase coding, Spread spectrum and echo hiding.

4.2.4 Video steganography

Image steganography consist of collection of pictures, sound used as a carrier of secret messages from one destination to another. The advantage of using video steganography is that large files can be transferred in a cover file of sound and pictures in disguise of being just a collection of pictures and sound to the intruders.

5 METHODOLOGY

The major concern of this work is to secure user data in the cloud during upload and download of data using Cryptography and Steganography and evaluate the performance of the system. The steps to be used in this work to achieve the security of data in the cloud is by first applying cryptography to convert the data into a scramble form that cannot be understood by unauthorized user using RSA encryption algorithm public key, conceal the data using Image Steganography and finally provide authentication to the data using RSA private key.

5.1 RSA Key Generation, Encryption and Decryption Process:

According to [37] RSA key generation, Encryption and Decryption are done using the following steps:

A. Key Generation

1. Choose two large prime no. p & q.
2. Calculate N = p * q
3. Calculate f (z) = (p-1) * (q-1) Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (z)) =1.
4. Calculate a number d such that d = e-1 mod f (n).

B. Encryption

5. Enter message to get cipher text. Cipher text c = mod ((message. ^e), N).

C. Decryption

6. The cipher text is decrypted by: Message=mod ((c.^d), N)

5.2 Proposed System

This work is aimed at improving cloud security system that will secure user data in the cloud using RSA algorithm as digital signature and Image Steganography. The working of RSA as digital signature as described in [10] is as follows:

1. Hash function is frame to create a message digest
2. For encryption, the public key generated using RSA algorithm is used to sign the document
3. For decryption, the private key generated using RSA algorithm is used to verified and decrypt the document.

Once the above is achieved, Image Steganography is then used to conceal the data in order to achieve a smooth transfer of data without drawing the attention of intruders. To have access to the concealed data, the data will be verified with the private key, on successful validation, the user will be able to extract the stegno data and decrypt the content of the data using the private key.

5.3 Working principle of the proposed system

A. Encryption Procedure

1. Create data to be sent to the cloud.
2. Generate public and private keys using RSA algorithm.
3. Create a message digest which will be used to sign the data created using any hash function technique.
4. Sign the data using the RSA public key generated.
5. Encrypt the sign data using the RSA public key generated
6. Conceal the data using image steganography.
7. Upload the data to cloud service providers.
8. Share the RSA public key to valid users for authentication.

B. Decryption Procedure

1. Extract the conceal data
2. Decrypt the data using the RSA private key generated
3. Authenticate and verify the document using RSA private key.
4. Have access and make use of the data.

5.4 Architecture of the proposed system

Figure1 Below shows the proposed diagrammatical workflow of the proposed system. The architecture shows an enhanced security technique using RSA as digital signature and image steganography used to secure data transfer in the cloud.

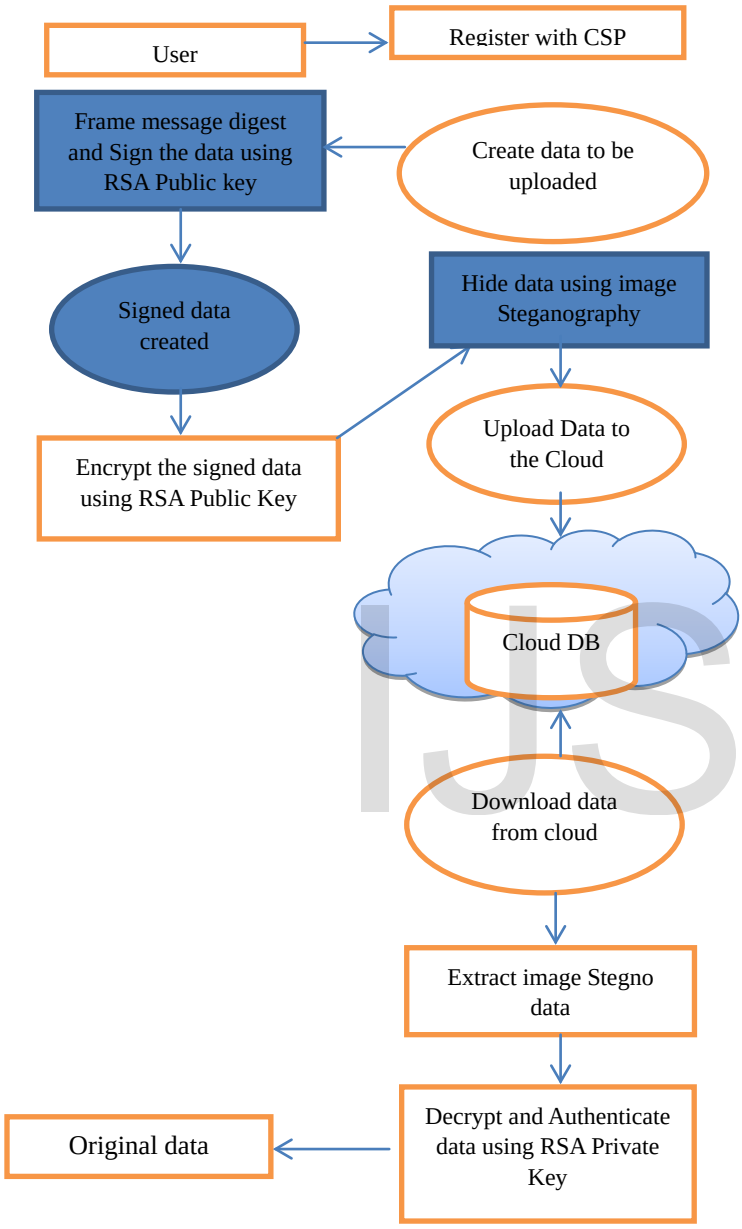

Fig1. Architecture of the proposed system

6 SIMULATION TOOLS

The proposed system will be implemented using java NetBeans IDE 8.0.2 programing environment to analyze the effectiveness of the algorithm and also to evaluate the performance of the system, on HP laptop System Corei (TM) i5-4200U, 2.30GHz CPU and 8GB RAM.

7 CONCLUSION AND FUTURE WORK

This work proposed a technique to protect user data when uploading and downloading the data from the cloud using RSA as digital signature and image steganography. The use of cryptography and steganography to secure data provides a strong security on data by transforming the data to unreadable form and concealing it from unauthorized users in order to achieve a secure communication in the cloud. Our proposed technique is considered to provide a strong security and secure transfer of data in the cloud. Our next work is to evaluate the performance of the system against other hybrid cloud security systems proposed by other researchers using different data types in order to measure its efficiency and resources consumed by the algorithms such as memory storage, network bandwidth, CPU processing time and power.

REFERENCES

[1] Abraham, L., Maribel, T., & Gebremedhn, M. (2015). Performance Analysis on the Implementation of Data Encryption Algorithms Used in Network Security. *International Journal of Computer and Information Technology, 4*(4).

[2] Arockiam, L., & Monikandan, S. (2013). Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(8).

[3] Ayushi. (2010). A Symmetric Key Cryptographuc Algorithm. *Intenational Journal of Computer Applications, 1*(15), 0975 - 8887.

[4] Bharwadj, A., Subrahmanyam, G., Avasthi, V., & Sastry, A. (2016). Security Algorithms for Cloud Computing. *International Conference on Computational Modeling and Security* (pp. 535-542). Elsevier B.V.

[5] Dhamija, A., & Dhaka, V. (2015). A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration. *International Conference on Green Computing and Internet of Things* (pp. 346-351). IEEE.

[6] Dubey, R., Saxena, A., & Gond, S. (2015). An Innovative Data Security Techniques Using Cryptography and Steganographic Techniques. *International Journal of Computer Science and Information Technologies, 6*(3), 2175-2182.

[7] Garima, S., & Naveen, S. (2014). Triple Security of Data in Cloud Computing. *International Journal of Computer Science and Information Technologies*, 5825-5827.

[8] Hariri, M., Karimi, R., & Nosrati, M. (2011). An introduction to steganography methods. *World Applied Programming, 1*(3), 191-195.

[9] Jasleen, K., & Deepankar, V. (2014). Steganography Techniques –A Review Paper. *International Journal of Emerging Research in Management &Technology, 3*(5), 132-135.

[10] Jasleen, K., & Sushi, G. (2015). Security in Cloud Computing using Hybrid of Algorithms. *International Journal of Engineering Research and General Science*.

[11] Kalyani, P. K., & Neha, V. N. (2016). Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security. *International Journal of Scientific Engineering and Applied Science*.

[12] Kamboj, P., & Bansal, E. L. (2016). A Review Paper on 3 Step Mechanism Using RSA, AES and MD5 to Improve the Security in

Cloud Environment. *International Journal of Advanced Research in Computer Science and Software Engineering, 6*(7), 389-392.

[13] Khatoon, A., & Ikram, A. A. (2014). Performance Evaluation of RSA Algorithm in Cloud Computing Security. *International Journal of Innovation and Scientific Research, 2*(1), 336-345.

[14] Mohsin, K., Sadaf, H., & Malik, I. (2013). Performance Evaluation of Symmetric Cryptography Algorithms: A Survey. *International Journal of Information Technology and Electrical Engineering, 2*(2).

[15] More, P., Temgire, K., Kamble, P., & Chavan, D. (2016). A Survey: Data Security in Cloud Computing Based on RSA. *International Engineering Research Journa, 2*(5), 1968-1970.

[16] Najib, A. k. (2013). Java Implementation and Performance Evaluation of SomeCryptographic Ciphers under WinXP and Linux Operating System Platforms. *Information and Knowledge Management*.

[17] Navneet, K., & Sunny, B. (2014). International Journal of Engineering Trends and Technology. *A Survey on various types of Steganography and Analysis of Hiding Techniques, 11*(8), 388-392.

[18] Neha, M. K. (2016). Enhanced Security using Hybrid Encryption Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering, 4*(7), 13001-13007.

[19] Omer, K. J., Safia, A., El-Sayed, M. E.-H., & Abdel-Badeh, M. S. (2013). Efficiency Of Modern Encryption algorithms in Cloud Computing. *International Journal of Emerging Technology In Computer Science, 2*(6).

[20] Pansotra, E. A., & Singh, E. S. (2015). Cloud Security Algorithms. *Internation Journal of Security and Its Application, 9*(10), 353-360.

[21] pant, V. k., Prakash, J., & Asthana, A. (2015). Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques. *In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on* (pp. 490-494). IEEE.

[22] Prince, J. (2012). Security Issues and their Solution in Cloud Computing. *International Journal of Computing & Business Research*.

[23] Rabi, P. P., Manas, R. P., & Suresh, C. S. (2011). Cloud Computing: Security Issues and Research Challenges. *International Journal of Computer Science and Information Technology & Security*.

[24] Rachna, A., & Anshu, P. (2013). Secure User Data in Cloud Compputing Using Encryption Algorithms. *Interanational Journal of Engineering Research and applications, 3*(4), 1022-1926.

[25] Ramalakshmi, S., & Rexy, J. (2017). Enhancing Cloud Security with Automatic Data Classification and Appropriate Encryption Algorithms. *International Journal of Innovative Research in Computer and Communication Engineering, 5*(1).

[26] Randeep, K., & Supriya, K. (2014). Analysis of Security Algorithms in Cloud Computing. *Internation Journal of Application or Innovation in Engineering & Management, 3*(3).

[27] Rupali, K., & Patil, A. (2015). Review Paper on Different Types of Steganography. *International Journal of Research in Electronics and Computer Engineering, 3*(2), 122-124.

[28] Sachdev, A., & Bhansali, M. (2013). Enhancing Cloud Computing Security using AES Algorithm. *International Journal of Computer Applications, 67*(9), 0975 – 8887.

[29] Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data Security Using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Applications,, 7*(6), 390-397.

[30] Shakeeba, S. K., & Tuteja, R. R. (2016). Cloud Security Using Multilevel Encryption Algorithms. *Internalnational Journal of Adance Research in Computer and Communication Engineering, 5*(1).

[31] Shirole, B. S., & Sanjay, T. (2014). Data Confidentiality in Cloud Computing with Blowfish Algorithm. *International journal of Emerging Trends in Science and Technology, 1*(1).

[32] Shivlal, M., Arti, S., Pradeep, S., Gautam, S. S., & Purohit, N. (2015). Performance Analysis of Encrption Algorithm in Cloud Computing. *Internation Journal of Computer Science and Engineering, 3*(2).

[33] Subhash, S. B., & Thakur, S. (2014). Data Confidentiality in Cloud Computing with Blowfish Algorithm. *International journal of Emerging Trends in Science and Technology*, 01-06.

[34] Sudha, M., & Monica, M. (2012). *Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography.* United States: World Science Publisher.

[35] Sunil, Y., & Kanishk, B. S. (2015). Evaluation and Review of Security Algorithm on Cloud Computing Environment. *International Journal of Innovative Research in Computer and Communication Engineering, 3*(4).

[36] Sunita, R., & Ambrish, G. (2012). Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints. *International Journal of Computer Science and Information Technologies*, 4302-4304.

[37] Varsha, & Chhillar, R. S. (2015). Data Hiding Using Steganography and Cryptography. *International Journal of Computer Science and Mobile Computing, 4*(4), 802-805.

[38] Vinita, K., Ali, S. I., & Sharma, N. (2016). Hybrid Approach of Chrptographic Algorithms in Cloud Computing. *International Journal Emaerging Technology and Advanced Engineering*.

[39] Waleed, A.-M., & Chunlin, L. (2016). User Privacy and Security in Cloud Computing. *International Journal of Security and Its Applications, 10*(2), 341-352.