ISSN: 0976-3104
ISSUE: COMPUTER SCIENCE

ARTICLE

CLOUD COMPUTING DATA SECURITY USING ENCRYPTION ALGORITHMS

Kumar Rithvik[1], Simran Kaur[1], Shilpa Sejwal[1], Priti Narwal[1], Prateek Jain[2]*

[1]*Department of Computer Science & Engineering, Manav Rachna International Institute of Research & Studies, Faridabad, INDIA*

[2]*Accendere Knowledge Management Services Pvt. Ltd., INDIA*

ABSTRACT

The "cloud" is a set of different types of hardware and software that work collectively to deliver many aspects of computing to the end-user as an online service. Cloud Computing is the use of hardware and software to deliver a service over a network. With cloud computing, users can access files and use applications from any device that can access the Internet. There are a wide range of companies and industry verticals that use cloud computing such as Amazon and Google. While no storage solution is 100% safe, cloud storage providers can offer a safer and more accessible place for companies to store data than traditional computing methods. As Cloud computing has emerged as a new technology, it has also created new challenges such as data security, data ownership and trans-code data storage. In this paper we have discussed about cloud computing security issues, challenges that CSP (cloud service provider) face and study various security algorithms.

KEY WORDS
Algorithms: RSA, Diffie Hellman, DSA AES ,DES, Triple DES, Blowfish, Cloud Computing, Data Security

Received: 2 April 2019
Accepted: 26 May 2019
Published: 16 June 2019

***Corresponding Author**
Email:
Prateek.jain@accendere.co.in

INTRODUCTION

Cloud Computing is an important concept in computer development. It refers to the use of computing capacity, storage of computers and servers in the world over the Internet. It provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications [1]. Characteristics of cloud computing includes on-demand self-service, broad network access and resource pooling, rapid elasticity. Cloud systems automatically control and optimize resource use by a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts) [2]. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Such cloud services are deployed in various ways which includes Software-as-a-Service (SaaS): which refers to software available on demand, it is based on multi-tenant architecture. Software like word processor, CRM (Customer Relation Management), etc. or application services like schedule, calendar, etc. are executed in the –cloudll using the interconnectivity of the internet to do manipulation on data. Custom services are combined with3rd party commercial services via Service oriented architecture to create new applications [3]. It is a software delivery for business applications like accounting, content delivery, Human resource management (HRM), Enterprise resource planning (ERP) etc on demand on pay-as-you go model. Another method to deploy cloud is Platform-as-a-Service (PaaS): This layer of cloud provides computing platform and solution stack as service [4]. Platform-as-a-Service provides the user with the freedom of application design, application development, testing, deployment and hosting as well as application services such as team collaboration, web service integration and database integration, security, scalability, storage, persistence, state management, application versioning, without thinking about the underlying hardware and software layers by providing facilities required for completion of project through web application and services[5].Cloud can also be deployed as Infrastructure-as-a-Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as as service. Instead of purchasing servers, software, data centre space or network equipment, clients can buy these resources as outsourced service. In other words the client uses the third party infrastructure services to support its operations including hardware, storage, servers [6]. Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter [7]. Now the clouds can be of three types Private cloud, Public cloud and Hybrid cloud. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. Only the organization and designated stakeholders may have access to operate on a specific Private cloud [8]. A public cloud is a model which allows users access to the services and infrastructure and are provided off-site over the Internet. It'stypically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization [9]. Public clouds are managed by third parties or vendors over the Internet. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. However, security and governance issues must be well planned and ample security controls was put in place. A new concept combining resources from both internal and external providers will become the most popular choice for enterprises. A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds [10]. Hybrid clouds offer more flexibility than both public and private clouds. Specifically, they provide tighter control and security over application data compared to public clouds, while still facilitating on-demand service expansion and contraction. On the down side, designing a hybrid cloud requires carefully determining the best split between public and private cloud components [11].

IIOAB JOURNAL
ISSN: 0976-3104

Security in cloud computing involves concepts such as network security, equipment and control strategies deployed to protect data, applications and infrastructure associated with cloud computing. An important aspect of cloud is the notion of interconnection with various materials which makes it difficult and necessary securing these environments. Security issues in a cloud platform can lead to economic loss, also a bad reputation if the platform is oriented large public and are the cause behind the massive adoption of this new solution. The data stored in the cloud for customers represents vital information. This is why the use of such data by an unauthorized third party is unacceptable. There are two ways to attack data in Cloud [5]. One is outsider attack and the other is insider attack. The insider is an administrator who can have the possibility to hack the user's data. The insider attack is very difficult to be identified. So the users should be very careful while storing their data in cloud storage [9]. Hence, the need to think of methods that impede the use of data even though the data is accessed by the third party, he shouldn't get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage. Security allows the confidentiality, integrity, authenticity and availability of information [7]. The development of technologies and their standardization makes available a set of algorithms and protocols for responding to these issues [12].

The objective of this paper is to analyze data encryption algorithm for security purpose in cloud computing. The rest of the paper is organized in the following way. Section 2 deals with Symmetric Algorithms including DES, BLOWFISH, AES, Triple DES and Section 3 deals with Asymmetric Algorithms including RSA and Diffie-Hellman in section 3 of the paper.

RELATED WORK

A brief review of latest technology used for security in cloud computing has been presented. Thakur and Kumar provide a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of these parameters: speed, block size, and key size [1].

Seth et al. performs comparative analysis of three algorithm; DES, AES an RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool is used for conducting experiments. Experiments results are given to analyses the effectiveness of each algorithm [14].

The comparative analysis of five algorithm; DES, 3DES, AES, UMARAM and UR5 Algorithm, considering certain parameters such as throughput, encryption time and power consumption has been performed by Pavithra, & Ramadevi [5]. A cryptographic tool is used for conducting experiments. The experimental results show the superiority of our UR5 encryption algorithm over other algorithms in terms of the power consumption, processing time, and throughput [4].

Shaina Arora et al. design an algorithm to merge both enhanced RSA algorithm and El-Gamal algorithm to provide user with a higher level of data security. The enhanced RSA algorithm enables faster encryption and decryption process and generating public and private key faster than the original RSA [8].

The implementation of Data Encryption Standard algorithm, which is one of the symmetric key cryptography algorithms. The m file DES. m is created and the two functions encrypt and decrypt () are called into this file. This m file DES. m gives the time required for encryption and decryption in seconds for the entered text [7].

The comparative study of various cryptographic algorithms like AES, DES, RSA, Blow Fish, Elliptic Curve, SHA and MD5 and give a proper direction to the users for use of proper algorithm for securing of data in cloud computing environment [12].MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time.

The comparison between three symmetric key cryptographic techniques namely as DES, AES and Blowfish algorithms in terms of time and security by using image simulation. Based on the image files used and the experimental result it was concluded that Blowfish algorithm consumes least encryption time and DES consume maximum encryption time. We also observed that Decryption of Blowfish and AES algorithms is better than DES algorithm [9-11].

The conventional algorithms, based on their benefits and drawbacks has been discussed in next section. We additionally have in comparison the significance of each these cryptographic techniques. This paper also offers an appropriate future opportunity related to these cryptographic techniques.

Md. Alam Hossain et al. describes the basic characteristics (Key Length, Block size) of symmetric (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, El-Gamal, Paillier), Hashing (MD5, MD6, SHA, SHA256) algorithms. Also we implemented five well- known and widely used encrypt techniques like AES, DES, BLOWFISH, DES, RC4, RSA algorithms and compared their performance based on the analysis of their encryption and decryption time for different file sizes in the local system [7].

IIOAB JOURNAL
ISSN: 0976-3104

Kapoor et al. proposed a hybrid cryptographic technique for improving data security during network transmission is proposed and their implementation and results are reported. The proposed secure cryptographic technique promises to provide the highly secure cipher generation technique using the RSA, DES and SHA1 technique [11].

This paper discussed well-known cryptographic algorithms and also demonstrates the basic differences between the existing encryption techniques. Regardless of the mathematical theory behind an algorithm, the best algorithm are those that are well-known and well-documented because they are well- tested and well-studied.

EXISTING ALGORITHMS FOR SECURITY

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using ―the keyll and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys-private and public keys are used. Public key is used for encryption and private key is used for decryption.

Symmetric algorithms

This section deals with the symmetric algorithms. Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link [13].

Data encryption standard

The Data Encryption Standard (DES) is a block cipher. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is the block cipher—an algorithm that takes a fixed-length string of plain text bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits [14]. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

The advantages of DES lie on two facts:

- 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.
- 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.

Algorithm: functionDES_Encrypt (M, K) where M = (L, R) M IP(M)
For round 1 to 16 do Ki SK (K, round)
L Lxor F(R, Ki) swap(L, R) end swap(L, R) M IP-1 (M)
return M End

The weakness has been found in the design of the cipher:

- Two chosen input to an S-box can create the same output.
- The purpose of initial and final permutation is not clear.

Blowfish

This was developed in 1993 for the replacement of DES. It is one of the most common public algorithms provided by Bruce Schneier. As Blowfish is a symmetric algorithm, the same keys are used for decryption as well as encryption, the only difference is that the input to the encryption is plaintext, for decryption the input is cipher text. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this because of the size of cipher text as it involves the whole plain text and convert the same text in cipher text. Blowfish encrypts 64-bit blocks with a variable length key of 128-448 bits [15-16]. According to Schneier, Blowfish was designed with the followings objectives in mind: fast- Blowfish encryption rate on 32-bit microprocessors is 26 clock cycles per byte, compact- Blowfish can execute in less than 5 kb memory, simple-Blowfish uses only primitive operation -s, such as addition, XOR and table look up, making its design and implementation simple, secure- Blowfish has a variable key length up to maximum of 448-bit long, making it both secure and flexible[17].

IIOAB JOURNAL
ISSN: 0976-3104

Blowfish suits applications where the key remains constant for a long time (e.g. Communications link encryption), but not where the key changes frequently (e.g. Packet Switching).

Algorithm:

Divide x into two 32-bit halves: xL, xR For i = 1to 16:
XL= XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR Next I
Swap XL and xR (Undo the last swap.) xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

Blowfish is one of the fastest block ciphers in general use, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers. This prevents its use in certain applications, but is not a problem in others, such as SplashID. In an application, it's actually a benefit especially the password-hashing method used in Open BSD uses an algorithm derived from Blowfish that makes use of the slow key schedule. Blowfish is not subject to any patents and is therefore freely available for anyone to use. This has contributed to its popularity in cryptographic software.

The disadvantages of Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel. Each pair of users' needs a unique, so as number of users increase, key management becomes complicated. For example, N(N-1)/2 keys required. Blowfish can't provide authentication and non-repudiation as two people have same key. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput.

Advanced encryption standard

AES (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES in 1997. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the charactes 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[18].

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. This algorithm is fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs submitted. The criteria for choosing the AES algorithm includes security, cost, implementation [19].Some of the advantages of AES are:

- AES is more secure (it is less susceptible to cryptanalysis than 3DES).
- AES supports larger key sizes than 3DES's 112 or 168 bits.
- AES is faster in both hardware and software.
- AES's 128-bit block size makes it less open to attacks via the birthday problem than 3DES with its 64-bit block size.

Algorithm :

Cipher(byte() input, byte() output)
{ byte(4,4) State;
copy input() into State() AddRoundKey for (round = 1; round < Nr-1; ++round)
{SubBytesShiftRowsMixColumnsAddRoundKey }
SubBytesShiftRowsAddRoundKey copy State() to output()
}

Triple DES

In cryptography, Triple DES (3DES), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of by increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.
Some of the advantages of 3DES are:

- AES in Galois/Counter Mode (GCM) is challenging to implement in software in a manner that is
- both performant and secure.
- 3DES is easy to implement (and accelerate) in both hardware and software.
- 3DES is ubiquitous: most systems, libraries, and protocols include support for it.

IIOAB JOURNAL
ISSN: 0976-3104

Algorithm:

A naive approach to increase strength of a block encryption algorithm with short key length (like DES) would be to use two keys (K1, K2) instead of one, and encrypt each block twice: EK2(EK1(plaintext)).
If the original key length is n bits, one would hope this scheme provides security equivalent to using key 2n bits long. Unfortunately, this approach is vulnerable to meet-in-the-middle attack: given a known plaintext pair (x, y), such that y = EK2(EK1(x)), one can recover the key pair (K1, K2) in ~2n steps, instead of ~22n steps one would expect from algorithm with 2n bits of key[20].

Therefore, Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

cipher text = EK3(DK2(EK1(plaintext)))

I.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3. Decryption is the reverse:

plaintext = DK1(EK2(DK3(cipher text)))

I.e., decrypt with K3, encrypt with K2, then decrypt with K1. Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option.

Asymmetric algorithms

This section deals with the asymmetric algorithms. Asymmetric algorithms (public key algorithms) use different keys for encryption and decryption, and the decryption key cannot (practically) be derived from the encryption key. Asymmetric algorithms are important because they can be used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private.

RSA

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone. How RSA is going to work in cloud environment is explained as: RSA algorithm is used to ensure the security of data in cloud computing. In RSA algorithm we have encrypted our data to provide security. The purpose of securing data is that only concerned and authorized users can access it[20-21]. After encryption data is stored in the cloud. So that when it is required then a request can be placed to cloud provider. Cloud provider authenticates the user and delivers the data to user. As RSA is a Block Cipher in which every message is mapped to an integer. In the proposed cloud environment, Public key is known to all, whereas Private Key known only to user who originally owns the data. Thus encryption is done by the cloud service provider and decryption is done by the cloud user or consumer. Once the data is encrypted with the Public key, it will be decrypted using the corresponding Private Key only.

Algorithm

Key Generation: KeyGen(p, q) Input: Two large primes – p, q Compute n = p .q
φ (n) = (p - 1)(q - 1)

Choose e such that gcd(e, φ (n)) = 1 Determine d such that e .d ≡ 1 mod φ (n) Key: public key = (e, n)
secret key= (d, n)

Encryption: c = me mod n where c is the cipher text and m is the plain text

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.

IIOAB JOURNAL
ISSN: 0976-3104

Diffie-hellman

The Diffie–Hellman key exchange scheme was first published by Whitfield Diffie and Martin Hellman in (1976) [22]. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. This method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over aninsecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The algorithm is itself limited to the exchange of keys. The Diffie–Hellman key exchange algorithm depends for its effectiveness on the difficulty of computing discrete logarithms [15-17]. Key exchange Algorithm Let us assume the A and B want to agree upon a key to be used for encryption / decrypting messages that would be exchanged between them.
The Diffie-Hellman key exchange algorithm works as follows:

Firstly, A and B agree on two large prime numbers n and g. These two integers need not be kept secret. A and B can use an insecure channel to agree on them.

A chooses another large random number x and calculates c such that c=g x mod n A sends the number c to B

B independently chooses another large random integer y and calculate d such that d=g y mod n B sends number d to A

A now compute the secrete key K1 as follows K1= d x mod n B now computes the secret key K2 as follows. K2=c y mod n

Some are advantages of Diffie-Hellman key exchange scheme are:

- The security factors with respect to the fact that solving the discrete logarithm is very challenging, and
- That the shared key (i.e. the secret) is never itself transmitted over the channel.

Some are advantages of Diffie-Hellman key exchange scheme are:

- The fact that there are expensive exponential operations involved, and the algorithm cannot be used to encrypt messages - it can be used for establishing a secret key only.
- There is also a lack of authentication.
- There is no identity of the parties involved in the exchange

Digital signature algorithm

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.[22-23] A digital signature algorithm (DSA) typically consists of three algorithms: A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key a signing algorithm that, given a massage and a private key, produces a signature. A signature verifying algorithm that, gives a massage, public key and a signature, either accept or reject the massages claim to authenticity [23].

Key generation

Select a prime q of 160 bits
Choose 0≤t≤8, select 2511+64t<p<2512+64t with q/p-1 Select g in Zp and a=g(p-1)/q mod p.α≠ 1
Select 1≤ a ≤ q-1, compute y= α b mod p. Public key (p,q, α ,y) private key a
Signing

Select a random integer k, 0<k< q.
Compute r= (α k mod p) mod q. Compute k-1 mod q.
compute s=k-1*(h(m)+ar) mod q. Signature=(r,s).

Verification :

Verify 0<r<q and 0<s<q, if not, invalid. Compute w=s-1 mod q and h(m).
Compute u1=w*h(m) mod q. u2=r*w mod q. Compute v=(α u1 yu2 mod p)mod q.
Valid if v=r.

The following are the advantages of using digital signatures:

- Speed: Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.

IIOAB JOURNAL
ISSN: 0976-3104

- Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.
- Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.
- Authenticity: An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.

The following are the disadvantages of digital signatures:

- Expiry: Digital signatures, like all technological products, are highly dependent on the technology it is based on. In this era of fast technological advancements, many of these tech products have a short shelf life.
- Certificates: In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities.
- Software: To work with digital certificates, senders and recipients have to buy verification software at a cost.
- Law: In some states and countries, laws regarding cyber and technology-based issues are weak or even non-existent. Trading in such jurisdictions becomes very risky for those who use digitally signed electronic documents.

CONCLUSION

Cloud computing has many advantages over traditional storage system but there are still problems concerning security that need to be solved. Security is a major requirement in cloud computing while we talk about data storage If we can eliminate this security issue, the future is going to be on Cloud for large as well as small companies. In this paper, we have suggested some solutions that allow storage of data in an open cloud. Data security is ensured by our algorithms such as symmetric and asymmetric algorithms. The symmetric encryption technique and the asymmetric encryption technique are important in encryption of sensitive data. Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, it has been found that AES algorithm uses least time to of execution. RSA consumes longest memory size and encryption time. Blowfish algorithm has least memory requirement. DES algorithm consumes least encryption time. Our future will be considering some problems related to existing security algorithms and implement a better version of DES, 3DES, AES, RSA, IDES, Blowfish.

CONFLICT OF INTEREST
There is no conflict of interest.

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None.

REFERENCES

[1] Thakur J, Kumar N. [2011] DES, AES and Blowfish: Symmetric key cryptography algorithms simulation-based performance analysis. International journal of emerging technology and advanced engineering, 1(2):6-12.
[2] Harinath D, Murthy MR, Chitra B. [2015], Cryptographic methods & performance analysis of data encryption algorithms in network security. International Journal of Advanced Research in Computer Science and Software Engineering, 5(7):680-8.
[3] Manju RD. [2015] Sudesh Kumar. Analysis on Different Parameters of Encryption Algorithms for Information Security International Journal of Advanced Research in Computer Science and Software Engineering, 5(8):104-108.
[4] Adekanmbi OO, Omitola OO, Oyedare TR, Olatinwo SO. [2015] Performance Evaluation of Common Encryption Algorithms for Throughput and Energy Consumption of a Wireless System. Journal of advancement in engineering and technology, 3(1):1-8.
[5] Pavithra S, Ramadevi E. [2012] Study and performance analysis of cryptography algorithms. International Journal of Advanced Research in Computer Engineering & Technology, 1(5):82-86.
[6] Kashyap S, Madan N. [2015] A review on: Network security and cryptographic algorithm. International Journal of Advanced Research in Computer Science and Engineering, 5(4):1414-8.
[7] Hossain MA, Hossain MB, Uddin MS, Imtiaz SM. [2016] Performance Analysis of Different Cryptography Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3):40-52.
[8] Arora S. [2015] Enhancing Cryptographic Security using Novel Approach based on Enhanced-RSA and Elamal: Analysis and Comparison. International Journal of Computer Applications, 112(13):12-19.
[9] Kahate A. [2013] Cryptography and network security, Tata McGraw-Hill Education.
[10] Laser JS, Jain V. [2016] A Comparative Survey of various Cryptographic Techniques. International Research Journal of Engineering and Technology (IRJET), 3(03):11-17.
[11] Kapoor V, Yadav R. [2015] A Hybrid Cryptography Technique for Improving Network Security. International Journal of Computer Applications, ISSN: 0975–8887, 3(2):45-51.
[12] Wollinger T, Guajardo J, Paar C. [2003] Cryptography in embedded systems: An overview, proceedings of the Embedded World 2003 Exhibition and Conference. 735-744.
[13] Devi A, Sharma A, Rangra A. [2015] Performance Analysis of Symmetric Key Algorithms: Des, Aes and Blowfish for

Image Encryption and Decryption. International Journal of Engineering and Computer Science, 4(6):6-12.
[14] Seth SM, Mishra R. [2011] Comparative Analysis of Encryption Algorithms for Data Communication, 1(1):4-9.
[15] Dandalis A, Prasanna VK, Rolim JD. [2000] A comparative study of performance of AES final candidates using FPGAs, International workshop on cryptographic hardware and embedded systems Aug 17. Springer, Berlin, Heidelberg. 125-140.
[16] Spanos GA, Maples TB. [1995] Performance study of a selective encryption scheme for the security of networked, real-time video. In Computer Communications and Networks, 1995. Proceedings. Fourth International Conference on IEEE, 2-10.
[17] Elminaam DSA, Abdual-Kader HM, Hadhoud MM. [2010] Evaluating the performance of symmetric encryption algorithms. IJ Network Security, 10(3):216- 222.
[18] Mandal PC. [2012] Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. Journal of Global Research in Computer Science, 3(8):67-70.
[19] Singh L, Bharti RK. [2013] Comparative performance analysis of cryptographic algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 3(11):43-52.
[20] Fujisaki E, Okamoto T. [1999] How to enhance the security of public-key encryption at minimum cost. In International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, 53-68.
[21] Kaushik S, Singhal A. [2012] Network security using cryptographic techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 2(12):16-22.
[22] Kadam KG, Khairnar PV. [2015] Hybrid RSA-AES Encryption for Web Service. International Journal of Technical Research and Applications, 51-56.
[23] Nadeem A, Javed MY. [2005] A performance comparison of data encryption algorithms. In Information and communication technologies. ICICT. First international conference on IEEE, 84-89.