RESEARCH ARTICLE OPEN ACCESS

The Classification and Analysis of Security Algorithms in Cloud Computing Environment

[1]D.Pharkkavi, [2]Dr.D.Maruthanayagam
1Research Scholar, Periyar University, Salem, Tamilnadu, India.
2Assistant Professor, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.

Abstract:

Cloud computing basically comes to focus on IT, a way to increase scope or add potentiality on the fly without spending in new infrastructure, training new personnel, or licensing new software. It encircles any subscription based or pay-per-use service that, in real time over the Internet, extends its existing capabilities. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (Pass), or software as a service (SaaS). Microsoft Azure and Google App Engine are the examples of platform as a service. The fast growth in field of "cloud computing" also increases rigorous security concerns. In cloud computing, security is the major issue. Due to this reason, the different algorithms have been proposed so far by researchers to provide security to critical data. This paper gives an obvious classification and analysis to those existing security algorithms in Cloud Computing Environment.

Keywords — **Cloud Computing, Security, DES, RC5, Blowfish, RSA**

I. INTRODUCTION

Cloud computing because of its broadband Internet, shared pool of the resources, flexible configuration, On-demand services and by service charges and other unique advantages, and in various industrial applications rapid rise. For business users, can significantly reduce the computational and storage. Maintenance costs for individual users and the calculation information stored by the discharge. In the cloud, reducing the number of their limited storage and computing resources arising Constraints. Cloud computing providers with their strong economic and technological strength; Guarantee a high degree of reliability of the cloud under law and regulations. In cloud computing, the user is placed in the cloud server data and meter Considered out of control, the data are protected, whether computing tasks determine the correct execution or not. Hence the need to design appropriate security protection mechanisms for protect user data confidentiality, integrity, availability, and the need to make cloud services.

The method of execution is credible, or can occur through accountability attack quickly determines where the problem lies. In a public cloud, a large number of users you can lease the resources in the cloud, and can lease the infrastructure to other use. Households want to provide services, or inevitable to communicate between the number of these users according to sharing. So between the cloud and more secure access to user needs and design for a Control mechanisms [1]. Because of the open nature of cloud computing and resource sharing special, emerged, as based on a common side channel attack based physical machines and a total denial of service attacks in the subnet and so on. To design new defensive measures to resist these attacks. In addition, it is more research [2] proposed to carry out the security services in the cloud, one can enough to enhance the capacity and processing power to update the security services, on the other hand can reduce the computational cost of the customer. This new security product is called "security that service (Security as a Service)". Mobile phone as a client of the situation because of its computing and storage capacity may very limit. At present, research includes anti-virus service [2], the certification, Safety testing and Digital Rights Management and so on.

Security Requirements of Cloud Computing

A. Confidentiality

In order to protect data privacy, data in the cloud should cipher text form, type storage, but the encryption method has brought on the overhead

operation, and therefore to calculate the cost to as little as possible to bring reliable data confidentiality; To protect the privacy of user behavior, cloud servers to ensure that users anonymous use of cloud resources and safety record data origin. Furthermore, in some applications, the server needs to be transported in a user data above count, and operation results are returned to the user in plain text format, thus enabling service is able to operate directly on top of the cipher text is an important demand side to. In the best case, the server any operation on the cipher text can be directly mapped to corresponding operations on the plaintext, this encryption method called fully homomorphism encryption [3]. If fully homomorphism encryption efficiently the realization of security, not only to protect the user's privacy, but also efficiency does not decrease. In the case of fully homomorphism encryption cannot be efficiently implemented, Lee with the same characteristics as a function of state protection of privacy, the cipher text based operation, but also is very important. In cloud computing, information retrieval is a very common operation make, and therefore supports the search cloud security encryption is an important requirement. Already some support for the search of encryption supports only single keyword search, and search results do not support the sorting and fuzzy search. Features for cloud computing, mesh studies include fuzzy search before, supporting the sort of search and multi-keyword search [4] and so on. If the operation cannot be performed on the cipher text, then any action by the user to be related to the data to be sent back to the user cipher text after the party decryption then, it will seriously reduce efficiency.

B. Data integrity

In a cloud-based storage services, such as Amazon Simple Storage Service S3, Amazon Elastic Block Store EBS, and Nirvana cloud storage Service, the need to ensure the integrity of the stored data. Several cloud based according stream processing, the main consideration is the complete data processing results detection and malicious service providers. In data storage, since users can not fully trust the cloud server will protect the integrity of their own data, so users need them integrity of the data for validation. Remote data integrity verification is a good way to solve this problem, it cannot download user data under the circumstances, based solely on the data to identify the challenges and server response code shall be able to verify the integrity of the data. The main source of data stream processing, the integrity verification requirements to user data processing service provider cloud mistrust. In this, under the case ensuring the integrity of the data processing results is essential.

C. Access Control

Cloud computing resources should stop the illegal users and other user's access to data or like, fine-grained control access to legitimate users, because this cloud server needs access to the user's behavior for effective verification. Its access control requirements include the following two aspects: (1) Network Access Control: refers to a cloud infrastructure between hosts each other access control. (2) Data access control: refers to the user data stored in the cloud access control. Access control data ensure that the operation of the user revocation method. For that, the user dynamically join the user can audit and other requirements also support.

D. Authentications

Existing authentication technologies include three categories: (1) based on the user holding secret certification; (2) hardware-based user hold (such as smart Card, U Shield, etc.) certification; (3) based on user biometric (eg fingerprint) Certification. Currently password authentication and X. 509 Certificate is a cloud products used widely considered authentication methods. In addition, the level of based authentication can achieve levels of between Multiple Clouds Identity Management. Multi-factor authentication can from the multiple features of the Client authentication; it is possible to provide enhanced security.

E. Credibility

In order to enhance the credibility of cloud computing and cloud storage services can start from two aspects. one hand is to provide accountability function of cloud computing, communication had achieved record operating information tracking and accountability malicious actions, such as [6] propose a cloud environment based on trust and fuzzy comprehensive evaluation unit trust management cloud System, based on credible mode service calls and feedback cloud services Type; the other is to build a trusted cloud

computing platform, through credible account count, secure boot, cloud gateways [5] and other technical means to be cloud computing.

F. Firewall Configuration Security

Infrastructure cloud, such as Amazon Elastic Compute Cloud [5], the cloud the virtual machine need to communicate, these communication between virtual machines are divided into communication and virtual machines and external communication. Control communication via firewall to achieve, and therefore the security of the firewall configuration is very important. If the firewall configuration problems, then the attacker is likely to use a port is not properly configured for a virtual machine to attack. Therefore, in the cloud calculations necessary to design the virtual machine firewall configurations safety of trial search algorithm.

G. Virtual Machine Security

Virtual machine technology to build cloud services architecture a large-scale user request and network resource allocation efficiency is widely used, but with this same when the virtual machine is also facing two aspects of security, on the one hand is a virtual machine safety oversight program, and on the other hand is a secure virtual machine images resistance. In a virtual infrastructure supporting technology into the cloud, virtual machines supervision software program is the highest authority on each physical machine, so it's safe there is no doubt of the importance of the whole. In addition, the use of third-party virtual released the case of machine images, virtual machine images whether to include malware or not.

II SECURITY ALGORITHMS

The main focus is on cryptography to make data secure when transmitted over the network. Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. In cryptography, encryption and decryption techniques are used. An encryption converts plaintext or message into cipher text and decryption extracts original message or plaintext from the same cipher text. Firstly, the information should be encrypted using the encryption algorithm in cryptography. Secondly, by using decipherment technique the receiver can read the original information. The figure shows some of the symmetric and asymmetric algorithms [7]:

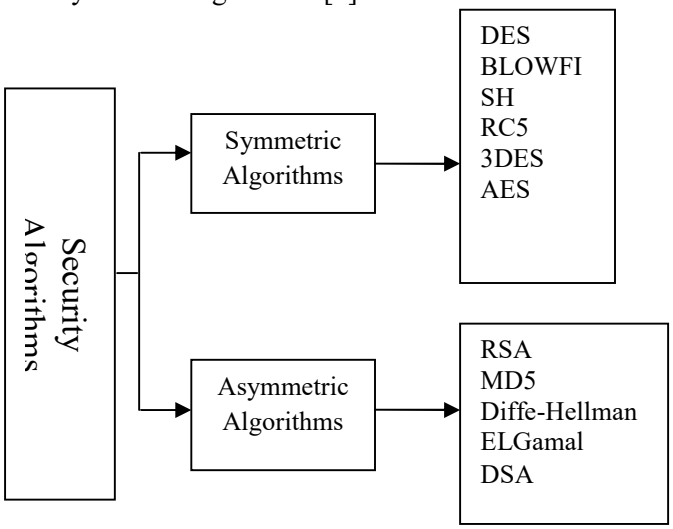

Figure 1. Security Algorithms

A) Symmetric Algorithms (private)

In Symmetric keys encryption or secret key encryption, one same key is used to encrypt and decrypt the data. Hence the key is kept secret. These algorithms do not consume an excessive amount of computing power. Symmetric algorithms are of two types: Block cipher (block of plaintext is encrypted) and Stream cipher (one bit at a time).

1) DES

DES stands for Data Encryption Standard and it was developed in 1977. It was the initial encryption standard to be recommended by authority NIST (National Institute of Standards and Technology). DES uses 64 bits key size with 64 bits block size. Since that time, several attacks and methods have witnessed the weaknesses of DES that made it an insecure block cipher. Two elementary features of cryptography Diffusion (Substitution) and Confusion (Permutation) rounds. In every round key and information bits are shifted, permuted, XORed. 64 bit plain-text is bimanual to initial permutation (IP).Then IP generates two halves left plain-text (LPT)and right plain-text (RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined. At the encoding site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decoding site, it takes a 64-bit cipher text and creates a 64 bit plaintext, and same 56 bit cipher key is used for both encoding and decoding. The encryption process is made of two permutations (P-

boxes), which we can call initial and final permutation, and sixteen Feistel rounds. The function f is made up of four sections [8]:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- 26 A straight P-box.

Algorithm:

Function DES_Encrypt (M, K) where M = (L, R)

M ⟵ IP(M)
For round1⟵ to 16 do
Ki ⟵ SK (K, round)
L ⟵ L xor F(R, Ki)
swap (L, R)
end
swap (L, R)
M ⟵IP-1(M)
return M
End

2) Blowfish

This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [8].

Algorithm:

Divide x into two 32-bit halves: x**L**, x**R**
For i = 1to 16:
XL= XL XOR P**i**
x**R** = F(X**L**) XOR x**R**
Swap X**L** and x**R**
Next i
Swap X**L** and x**R** (Undo the last swap.)
x**R** = x**R** XOR P**17**
x**L** = x**L** XOR P**18**
Recombine x**L** and x**R**

3) RC5

It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow. [9]

Algorithm:

A = A + S[0];
B = B + S[1];
for i = 1 to r do
A = ((A Xor B) <<< B) + S[2 * i]
B = ((B Xor A) <<< A) + S[2 * i + 1]
Next

4) **3DES**

This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics [8][10].

A quite simple way of increasing, the key size of DES is to use Triple DES, to guard it against attacks without the need to design a completely new block cipher algorithm. DES itself can be adapted and reused in a more secure scheme. Many former DES users can use Triple DES (TDES) which was described and analyzed by one of DES's patentees. It involves applying DES more times with two (2TDES) or three (3TDES) different keys as shown in figure 2. TDES is quite slow but regarded as adequately secure.

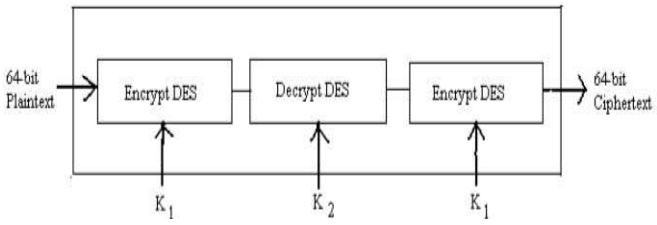

Figure 2. Encryption: Triple DES

Algorithm:

For j = 1 to 3
{
C**j,0** = IV**j**

```
        For i = 1 to nj
        {
                Cj,i = EKEY3 (DKEY2
        (EKEY1 (Pj,i Cj,i-1)))
                Output Cj,i
        }
}
```

5) AES

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively [11]. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128. Its algorithm is as follows:

1. Key Expansion
2. Initial Round
3. Add Round Key
4. Rounds
5. Sub Bytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
6. Shift Rows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
7. Mix Columns - a mixing operation which operates on the columns of the state, combining the four bytes in each column
8. Add Round Key - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9. Final Round (no Mix Columns)
10. Sub Bytes
11. Shift Rows
12. Add Round Key

Algorithm

```
        Cipher(byte[] input, byte[] output)
        {
                byte[4,4] State;
                copy input[] into State[]
        AddRoundKey
                for (round = 1; round < Nr-1;
        ++round)
                {
                        SubBytes ShiftRows
                MixColumns AddRoundKey
                }
                SubBytes ShiftRows
        AddRoundKey
                copy State[] to output[]
        }
```

B) Asymmetric Algorithms (public)

In Asymmetric keys, two keys are used: private and public keys. Public key is used to encode the data and private key is used to decode the data. Public key encryption is predicated on mathematical functions and intensive in computation. Encryption is the elementary tool for safeguarding the data. Encryption algorithm converts the data into scrambled form by using "the key" and solely user has the key to decode the information.

1) RSA

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

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the 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 can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1. Cloud service provider should give or transmit the Public-Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is C = me (mod n).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:

Decryption is the process of converting the cipher text (data) to the original plain text (data).

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

2) MD5 Algorithm

The **MD5** message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity [12]. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C, and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation.

3) Diffie-Hellman Key Exchange

In 1976, Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the use of the discrete logarithm problem. In this protocol sender and receiver will set up a secret key to their symmetric key system, using an insecure channel. To set up a key Alice chooses a random integer a [1; n] computes g^a, similarly Bob computes g^b for random b [1; n] and sends it to Alice. The secret key is gab, which Alice computes by computing $(g^b)^a$ and Bob by computing $(g^a)^b$. The important concepts on which the security of the Diffie-Hellman key exchange protocol depends are [11]:

- Discrete Logarithm Problem (DLP): If from g and g^a Eve, an adversary can compute a, then he can compute g^{ab} and the scheme is broken.

- Diffie-Hellman Problem (DHP): If from given the information g, g^a and g^b with or without solving the discrete logarithm problem, Eve can compute gab then the protocol is broken. It is still an open problem if DHP is equivalent to DLP.
- Decision Diffie-Hellman Problem (DDH): If we are given g; g^a; g^b and g^c, DDH is to answer the question, deterministically or probabilistically, Is ab = c mod n?

4) ElGamal

ElGamal encoding system is an asymmetric key encryption algorithm for public-key cryptography that relies on the Diffie-Hellman key exchange. It was delineated by Taher Elgamal in 1985.ElGamal encryption is used in the free GNU Privacy Guard software. The Digital Signature Algorithm is an alternative of the ElGamal signature scheme, which should not be confused with ElGamal encryption. The practical use of ElGamal cryptosystem is in a hybrid cryptosystem, i.e., the message itself is encoded with a symmetric cryptosystem and ElGamal is then used to encode the key used for the symmetric cryptosystem. This is done because asymmetric cryptosystems like Elgamal are slower than symmetric cryptosystems for the same level of security, so it is faster to encode the symmetric key (which most of the time is tiny if compared to the size of the message) with Elgamal and the message (which is randomly large) with a symmetric cipher. In this, each user has a private key x. Each user has three public keys: prime modulus p, generator g and public Y. ElGamal encoding is probabilistic encoding, i.e., the utilization of randomness in an encryption so that when we encrypt the plaintext, it can be encrypted to several potential cipher texts.

5) *DSA(Digital Signature Algorithm)*

The digital signature is analogous to the hand written signature. It is used for the authenticity of the document. Similarly, digital signature makes receiver belief that the sender is genuine and the receiving document is authentic. It must verify the author, date and time of the signature. After signing a message, the person cannot deny it. For signing a document 'private key' is used and 'public key' is generated for the signature verification. These keys-private and public are used for confidentiality.

The process of signature algorithm could be understood by the given figure. It shows how DSA works to generate and verified the signature.

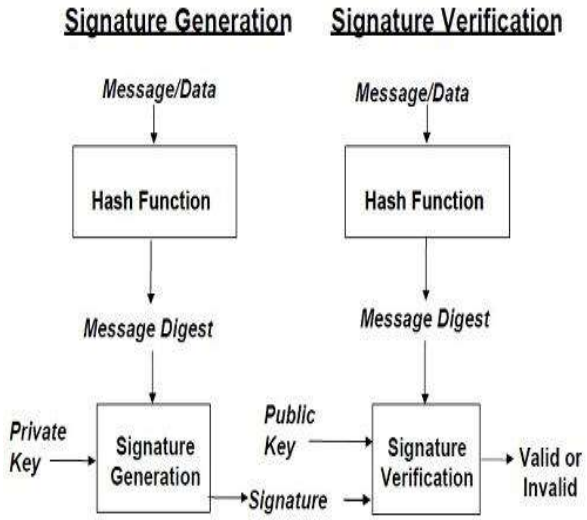

Figure 3. Digital Signature Scheme

In digital signature, the private and public keys of sender are used. The sender uses their private key and the receiver uses the private key of the sender. For encryption receiver's public key is used by sender and receiver uses his own private key to decrypt. Since the message are very long, it is not easy to sign a whole document itself in this case we sign a digest of the message. A secure hash function is used to create message digest-a condensed version of data. Now the signature got verified by the receiver.

CONCLUSION

In today's world, Cloud computing is rising as a new brand factor. There are several issues in cloud computing but the major issue concerns security issue. Many of the organizations are moving their data on the cloud but are concerned about security of their data. Thus cloud security is must which will be able to break the hindrance to the acceptance of the cloud by the organizations. In this paper, some existing security algorithms have been analyzed and discussed which

can be implemented to the cloud to provide security. As discussed so far there are many security algorithms which are currently available in cloud computing. Apart from these there is a great need to develop many more efficient algorithms to increase the security level of cloud computing environment.

REFERENCES

1. Shuai Zhang, Xuebin Chen , "The Comparison Between Cloud Computing and Grid Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM 2010).
2. Joshi Ashay Mukundrao , Galande Prakash Vikram "Enhancing Security in Cloud Computing" in Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online), Vol 1, No.1, 2011.
3. Murat Kantarcioglu, Alain Bensoussan, SingRu(Celine) Hoe, "Impact of security risks on cloud computing adoption," in forty-ninth annual allerton conference allerton house, uiuc, illinois, USA ,september 28 - 30, 2011.
4. Lamia Youseff, Maria Butrico, Dilma Da Silva, "Toward a Unified Ontology of Cloud Computing, in 2008 ,http://www.cs.ucsb.
5. Kunwadee, sripanidkulchai, sambit sahu, yaoping ruan, anees shaikh, and chitra dorai, "Are clouds ready for large distributed applications?," in IBM T.J. Watson Research Center.
6. Microsoft, "Comparing Web Service Performance: WS Test 1.1 Benchmark Results for.NET 2.0, .NET1.1, Sun One/ JWSDP 1.5 and IBM WebSphere6.0" http://www.theserverside.net/tt/articles/content/NET2Benchmarks.
7. Randeep Kaur,Supriya Kinger, 2014 Analysis of Security Algorithms in CloudComputing
8. Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Comparison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.
9. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
10. Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
11. M. Sudha, Dr. Bandaru Rama Krishna Rao, M. Monica —A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment, in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.
12. http://en.wikipedia.org/wiki/MD5

AUTHORS PROFILE

D.Pharkkavi received her M.Phil Degree from Tiruvalluvar University, Vellore in the year 2013. She has received her M.C.A Degree from Anna University, Chennai in the year 2012. She is pursuing her Ph.D Degree at Periyar University. Salem, Tamilnadu, India. Her areas of interest include Cloud Computing and Mobile Computing.

Dr.D.Maruthanayagam received his Ph.D Degree from Manonmanium Sundaranar University, Tirunelveli in the year 2014. He has received his M.Phil, Degree from Bharathidasan University, Trichy in the year 2005. He has received his M.C.A Degree from Madras University, Chennai in the year 2000. He is working as Assistant Professor, Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above 14 years of experience in academic field. He has published 1 book, 14 International Journal papers and 21 papers in National and International Conferences. His areas of interest include Grid Computing, Cloud Computing and Mobile Computing.