A COMPARATIVE ANALYSIS OF DES, AES AND RSA CRYPT ALGORITHMS FOR NETWORK SECURITY IN CLOUD COMPUTING

M.Kannan[1], Dr.C.Priya[2], S.VaishnaviSree[3]
[1]Research Scholar,[2]Associate Professor,[3]Research Scholar
[1]Department of Computer Science,
[1]School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India.
DOI: http://doi.one/10.1729/Journal.19997

Abstract: In the modern existence Data communication is a copious key to share the data from one faction to another faction through the nexus or transmission medium using few social media like Whatsapp, Messanger, facebookin between this,third factionmight obtain or retrieve the entropy or data. Cryptography is mainly used for authentication scope. For this equip Cryptography concept and algorithms are applied in an every social media (ex: twitter, Facebook, Instagram, LinkeIn), agencies, institutions, industries, etc. The view of DES, AES and RSA is one the major concern of this paper to explore, how these crypt theoriesare secure the data by the use of encryption and decryption.This paper takes a simple literature survey and also comparing the relationship between DES, AES and RSA crypt notion. In which they are one of the significant modules to secure and/or the messages using crypt file keys. In these, DES, AES and RSA concepts are used to protect the file with the service of encryption and decryption affair. The main intent of the DES, AES and RSA in cryptography is to secure the files.According to this all the key size is static.In this paper describes how cryptosystems are protecting the plaintext from the unsupported client.

IndexTerms **- DES, AES, RSA, Encryption, Decryption, Secret Key and Cryptography.**

I. INTRODUCTION

Cryptography is the proficiency used for secure communication without interfering third parties called opponent.Cryptographic algorithms are devising around **computational inclemency (hardness) notion.** Initially cryptography has supplementary paramount goals such as authentication, confidentiality, non-repudiation, integrity, availability. Advanced Encryption Standard(AES), Data Encryption Standard (DES), and Rivest, Shamir Adleman (RSA) is the main solicitude of this paper. And also in this paper have roughlycompare the concepts among AES, DES, and RSA. In which, Advanced Encryption Standard (AES) was nominated by Rijndael, is an enumeration for the encryption of electronic data.Which is a block cipher technique,the size of the key is 128-bits and also is a symmetric key. The key is a salient featureto excrement the file from one subscriber to another subscriber become confident. This is the major part of the cryptography globe.Whereas Data Encryption Standard (DES) was lodged by NBS/NIS (National Bureau of Standards/ National Institute of Standards) in1977. Which is also be a block cipher technique with 64-bit key. DES has a six rounds, using these roundsthe plaintext (original message) is metamorphosed into cipher text (other text), finally it will crown their tour to constitute the 64-bit plaintext. And Ron Rivest,AdiShamir Adlemanand Leonard Adleman(RSA) is the first public key cryptosystem in 1977. In the RSA, has separate encryption and decryption key which has disguised from one another. While comparing with other cryptographic algorithm, it is a pretty slow one.There are two componentsessential to encrypt the data by the use of cryptographic algorithm and akey. The Cryptographic algorithm kept a key as a stealthy so any other information should not be published.The key is a very large number that should be impossible to presume.

II. RELATED WORKS

To give more prospective about the comparability of those concepts, this section of the paper mostly discusses the literature survey and comparative analysis of cryptography. In this survey, we multitude figures about those cryptographic concepts for authentication and also protected from the third parties. According to these reason AES and DES are performed in many sites. Because which makes more confidence. Which means it will share the message only with a confident person.

III. CRYPTOGRAPHY BASIC MODEL

Cryptography involves provoke codes that allow information to be kept secret from the unauthorized user. All the information is kept secure and protected from the third party. For example, if Alice posts some paramount message to Bob, the third person might be read that information without the license of Alice and Bob. So the information might be unsecure. So that cryptography takes the charge to secure the secret. For this cryptography concept is used in many places.

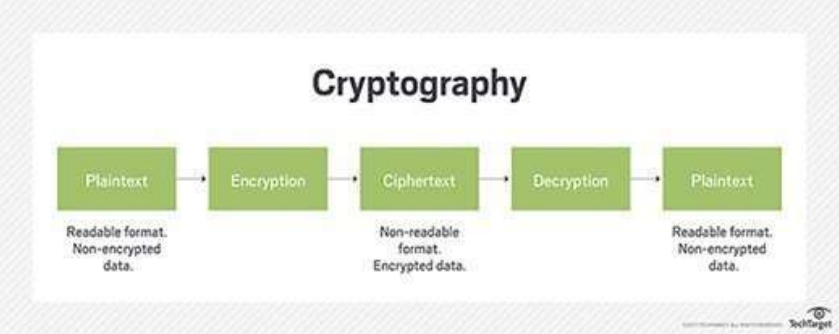

Fig 1: Cryptography Basic Function (Model)

In the above illustration cryptography basic function has some functions to change the message fromone text to other text using encryption and decryption standards for secure the information. According to this figure the plain text is changed into cipher text with the help of encryption, simultaneously the cipher text isagain converted into plaintext (User Readable Form) with the use of decryption.Thisis the basic concept of cryptography.Further, will move to the conceptsof DES, AES and RSA one after another viathis paper.Generally Cryptography has many types to protect the information; some of them are, Symmetric, asymmetric and block cipher & stream cipher cryptanalysis. These are some cryptography key which is also some types of cryptography, commonly used for file protection from the unknown person or from a third party.

IV.HYPOTHESIS OF AES, DES AND RSA

Cryptography uses many important concepts to protect the message from an unprotected user. From that some of them are discussed below:

4.1 STRUCTURE OF DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) was developed by the National Bureau of Standards (NBS) in 1970_s. The connotation of DES is to confer a standard and confident method to protect the vulnerable information and unclassified data.Each 64 bits of data is ingeminatefrom 1 to 16 times (which means 16 rounds). The following illustration is the Data Encryption Standard structure which carries 16 rounds to protect the original text from the unsubscribed user using S-boxes.

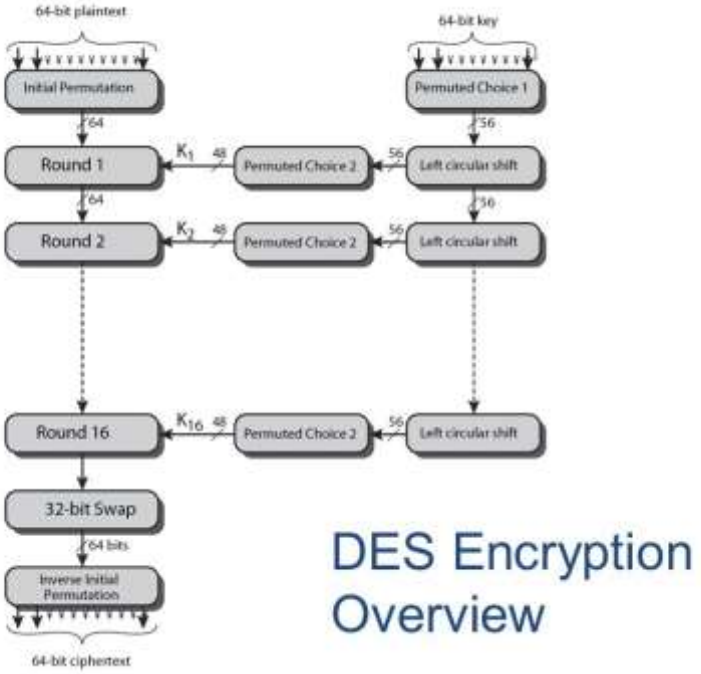

Fig 2: Structure of DES

Inthis diagram first the original message, which is 64-bit PT (Plain Text) was sent to the Initial Permutation after that the message will move on to all the 16-rounds of checking the PT in to bit by bit. Then it will complete their tour.Simultaneously the key will work, remember, 64 bit key is changed into 56-bit key since the actual size of a key is 56-bit. It will appertain through the Permuted function. After this process the key is converted into 48 bit, then it will be passedto the final round and vice versa. After the completion of 16 rounds the plain text is swapped into 32-bit. Finally the swapped message is sent to the Inverse Initial

Permutation (IP^{-1}), after the IP^{-1} function the 64-bit cipher text proclaims to the opponent. Both Permutation and Left Circular Shift uses the sub-key K_i at each and every level.This is the universal view of DES.

4.1.1 Solitary / Single Round of DES

The same procedure is as follows at every round which means every 16 rounds.

Steps:

a. Divide 64-bits into two 32-bit from both sides (left and right).

b. Then the R input is expanding to 48-bits by using Expansion Permutation (E).

c. Expansion Permutation (E) reveals the output in which they perform the XOR operation with key K_i.

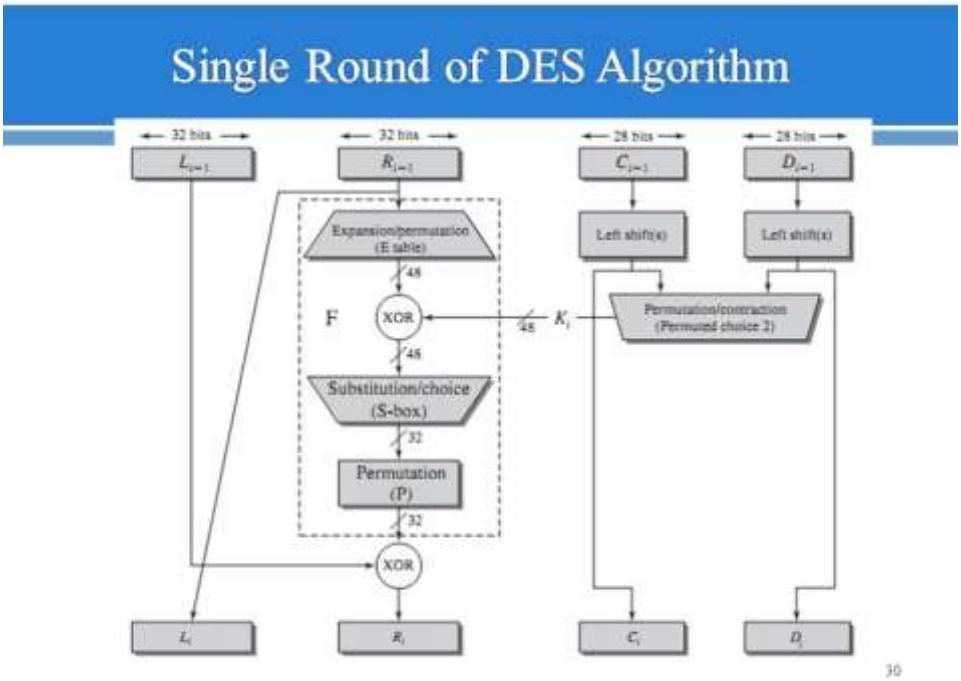

Fig 2(a): Single Round of DES

d. After the XOR operation,it produces the result which has passed to the S-box which givesas 32-bit output.

e. The Permutation Function (P) permuting the resultant value once again for the clarification.

f. Simultaneously 56-bit key will also be divided into two halves as 28-bits which give the performance using Left Circular Shift and Permutation, after thisit will reduce the size of the key and which spread the result into every round.

4.1.2 STRENGTH OF DES:

Some of the important strengths in DES are,

a. Data Encryption Standard has a strong avalanche effect.

b. Using this DES, Brute-force attack is not possible.

c. Timing attack is also difficult.

4.2 OVERVIEW OF ADVANCED ENCRYPTION STANDARD (AES)

AES is a symmetric block cipher also called as private, which uses the same key for the process of encryption and decryption. Advanced Encryption Standard (AES) was suggested by Rijndael. AES will encrypt and decrypt the block size of 128 bits using diverse cipher keys of 128,192, and 256 bits. Generally AES accommodates four alternate transformations such as Sub-Bytes, Shift Rows, Mix-Columns, and Add Round Key. In this paper focuses the concept around thecryptographic function in which how they are officiate in the network area. At first AES will monitor the block and key size of the text, then it will pertain the data into the AES algorithm. Which means it first evaluate the volume to insert the data. Data Encryption Standard (DES) involves six rounds to change from the plain text to cipher text, whereas, Advanced Encryption Standard (AES) involves 10 rounds to change from the plaintext to cipher text. This is the dissimilarity between these two systems.Each round is quite similar to convert the text. AES works under the encryption and decryption manner by the rule of Expand key. For encrypting, the algorithm will work from round 1 to 10. For decrypting, the algorithm will work in a reverse manner.Not only encrypted plain text128-bit key is also

constituted as square matrices of bytes. In this section the key is represented as words W_0 to W_{43}. Therefore 44 words, each word contains 4-bytes.Finally the key matrix is stored as words (Expanded Key).

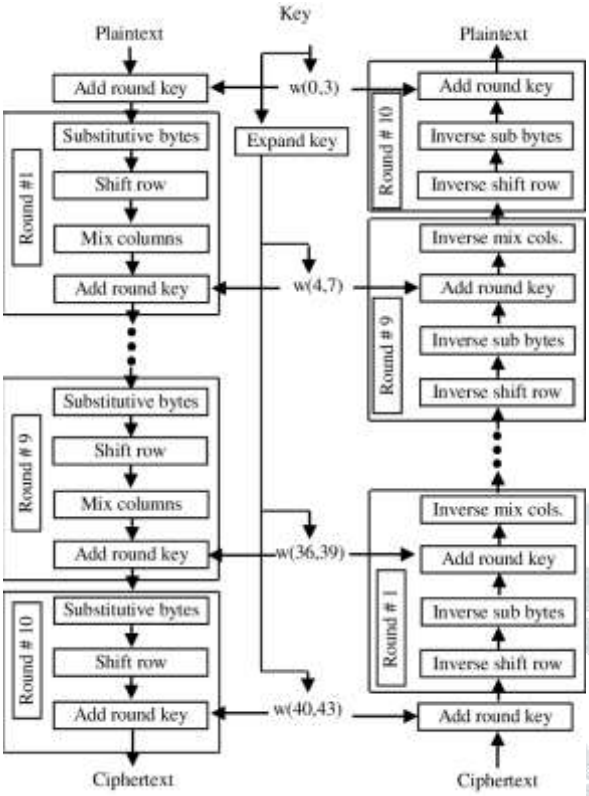

Fig 3: Block Diagram for AES Encryption and Decryption

The above figure (3) suppressesa few blocks or steps to do the encryption. AES takes 128-bit blocks as an input for encrypting the data or plaintext, which can be represented by square matrix. The particular matrix is copied into state array which performsome modification at each level of encryption.Which means the state array is replicated from an input matrix. After this process, the final result is sent to the out matrix. And also out matrix is a depot to save the output or the result.

A. Add Round Key: Add round key performs bitwise XOR operation between the state array and the resulting round key that is the output of the key expansion algorithm.

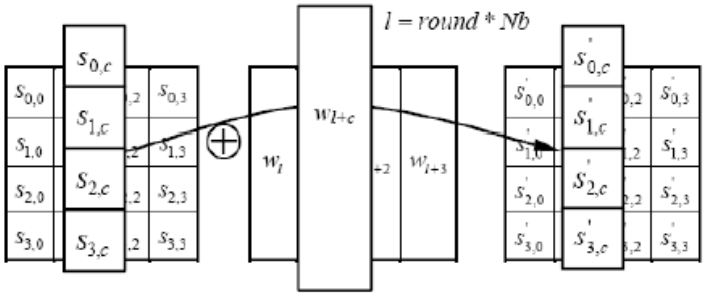

Fig 3(a): AES – Add Round Key

B. **Substitute Bytes:** Substitute Byte is also called as a Sub Bytes transformation which is one of the transformation technique which is a nonlinear byte substitution and also a simple table lookup technique. The implementation of this transformation is simple. Sub Bytes transformation is an S-Box which consist of 16*16 matrix in which the S-Box is used for both forward and inverse transformation.

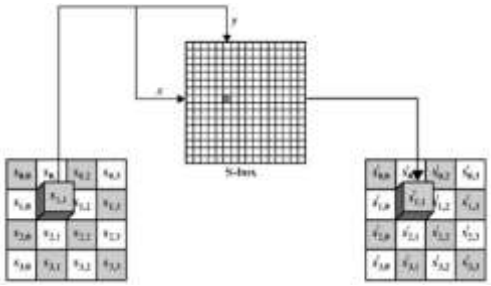

Fig 3 (b): AES – Sub Bytes

C. **Shift Row Transformation:** Which is nothing but, this transformation shifts the rows in a cyclic manner at each and every row to the left. It means each row is shifted to a different offset. Shift row transformation has some rules for shifting rows which are given below:

1. According the rule of Shift Row, the first step, the first row should not be shifted.
2. The shifting process will be started at the second step. In the second row the byte is shifting at one byte position to the left.
3. Likewise, the third row will be shifting at the two byte position to the left.
4. Fourth row is third position and viceversa.

Example: Shifting Rows at Row by Row

8A	**2F**	**16**	**32**
4D	**76**	**28**	**19**
DC	**17**	**0E**	**80**
A8	**DH**	**47**	**04**

↓

8A	**2F**	**16**	**32**
76	**28**	**19**	**4D**
0E	**80**	**DC**	**17**
04	**A8**	**DH**	**47**

D. **Mix Column Transformation:**This transformation usesa GF multiplication method for evaluating the bit values. Such transformation is also called as Galoi's Field. GF performs the XOR operation (which is the bitwise operator) to calculate all the bit values using 1-bit left shift operation.

4.2.1 AES ADVANTAGES AND DISADVANTAGES

Advantages:

1. When comparing to other method the process of AES has more speed.
2. S-Box is used to abolish the symmetric.
3. Comprehensibility of description.
4. More fastened, so no one cannot hack or attack the personal information.

Drawbacks:

1. It uses an excessively potty algebraic structure.
2. Implementing with software is much complicated.

4.3. APPLICATION OF RSA

RSA is the first public key cryptosystem which is also referred as a symmetric key cryptosystem in cryptography. RSA involves single round to encrypt and decrypt the original text or a message or plaintext. RSA was invented by Ronald Rivest (Ron Rivest), Adi Shamir, and Leonard Adleman in the year of 1978.It is an algorithm used for public key encryption.Few set of famous security system which is composed of 3 phases: 1) Prime Key Generation, 2) Encryption and 3) Decryption. The below figure is a basic encryption and decryption process which consist some key to encrypt or decrypt the message or to convert from plain to cipher by the use of cryptography algorithm.

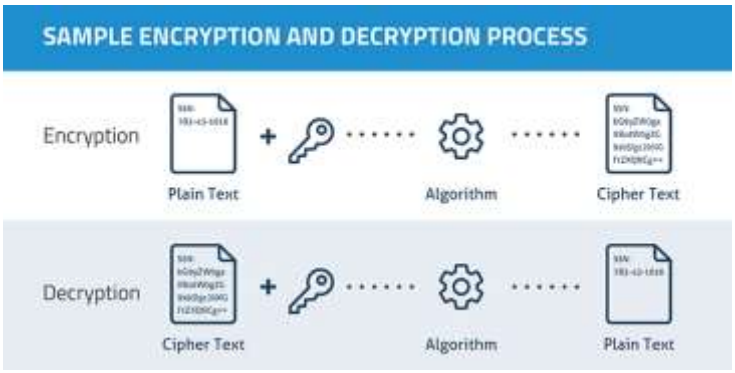

Fig 4 (a): Encryption and Decryption

The RSA system of encryption and decryption is portrayed in the succeeding sketch:

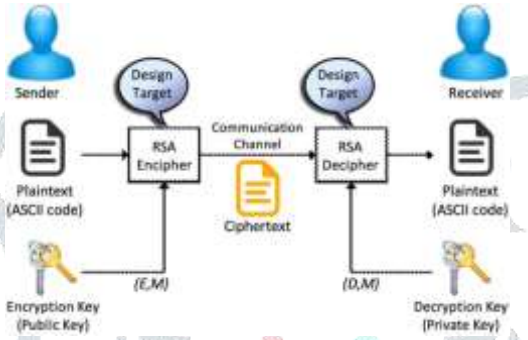

Fig 4 (b): Encryption and Decryption Using RSA

In the above sketch, the sender sends X the confidential message to receiver Y in between the process of encryption and decryption with the safeguard keys through the communication channel. At first, X sends the spontaneous message or plain text is sent to encipher which process the encryption operation using the sender's public key, after encrypting, the encrypted file is sent to decipher for the decryption process via the communication channel.In this (Encipher) process, the filemodifies into another type of text which is called cipher text. The RSA decipher will decrypt the cipher text using the sender's private key. Finally, the originalsafeguard decrypted plain text is received by the user Y.

4.3.1 ASYMMETRIC KEY

Asymmetric encryption is one of the discrete images of a crypto system. It has two sections, such as Encryption and Decryption. RSA uses one public and private key for securing and transferring the data from the unauthorized users. It is also called as key-pair. This pair of key is used to transferthe data within a time period. This function is also called as public-key encryption.

4.3.2 DIGITAL SIGNATURES

Digital Signatures (DS) are built from asymmetric cryptography and it can confer credence of manifest to radix, identification and designation of an electronic deed. Digital Signature is used to check or anauthenticate a message. Analogously, DS is a technique which binds an entity to the Digital Data. It will secure message from the third party. In this Digital Signature, hashing function is the one of the main prime to verifying a message and protect the document.Since, DS is invented by private key. Some of the DS significances are–

a. Message Authentication
b. Data Integrity
c. Non-Repudiation

4.3.3 RSA Advantages and Disadvantages

Advantages:

1. Safe and Secure
2. No one should nor crack the file

Disadvantage:

1. The RSA process might be slow while encrypting too long data.

V.SECURITY MANAGEMENT AREAS FOR CLOUD COMPUTING

Security Management (SM) includes functions that control and protect access to organization's resources, information, data, and IT services in order to ensure confidentiality, integrity, and availability. Security management functions are methods for authentication, authorization, encryption, etc. Unfortunately, the expanded definitions and standards around security management do not define a common set of security management areas.

The Security Management Infrastructure approach, which is also called Enterprise Security Management (ESM), is known to serve as comprehensive security architecture for our research. This approach of EU, NATO, the UK, and the USA, contains security management functions, such as Identity Management, Privilege Management Metadata Management, Policy Management, and Crypto Key Management. In addition, there are several sources that describe Cloud computing security areas. However, they differ in their compliance with necessary security management functional areas and collaboration aspects thatcan be used for a comprehensive Cloud security management For example, the management of meta-data or configuration management of security capabilities are not covered. Mainly they focus on Identity, Privilege, Access, and Crypto Key Management.Based on the presented sources above, we present the following ten security management areas for Cloud computing, that can be briefly described as follows:

Identity Management *is* the ability to confirm and manage the life cycle of an assured identity (human/device/process) Amalgamated Identity Management provides end users with secure access across multiple external applications through coalesce single sign-on.

Credential Managementis the ability to manage the life cycle of digital credentials. Examples of credentials include certificates, private keys, user IDs, and passwords. The credential management is also responsible for verifying the authenticity of credentials.

Attribute Managementis the ability to manage the assigned properties of entities. An attribute is a specification which defines a property of an entity. The key elements are: publishingof attribute requirements, support for user consent, and common attribute policies. Furthermore, it is responsible for requesting the new attribute and associated values from service upon attempts to access the service.

Privilege Managementis the ability to manage permissions to perform an action. It is designed to address the challenges of managing what people can access and giving control of that process to those in the departments who make the decisions.

Digital Policy Management (DPM) mitigates compliance and intellectual property risks through efficient and effective digital policy management. Itis the ability to generate, convert manage and replace digital policies. Digital policies are those that are in machine-specific languages and can be used to guide the behavior of systems in an automated or semi- automated manner.

Configuration Management (CM)is a field ofmanagement that focuses on establishing and maintaining consistency of a system or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. It manages the security-related configuration items, such as defining, controlling, ordering, and loading of configuration data for services.

Cryptographic Key Managementencompasses all of the activities and to provide protocol security services, especially integrity, authentication and confidentiality.

Metadata Managementinvolves storing information about other information. It is an important part of enterprise information management (EIM). It is the ability to generate and manage all security-relevant metadata schema and values over their life-cycle.

Audit Managementis the ability that establishes auditable security-relevant events. Management audits are often necessitated by major changes in a business. Some of the events that call for a management audit are top management changes, mergers and acquisitions, and succession planning. Analysis and assessment of competencies and capabilities of a company's management in order to evaluate their effectiveness, especially with regard to the strategic objectives and policies of the business.

SM Information Managementis the ability to gather and manage security-relevant information of Cloud services (such as region, time, etc.) that are not a native component of the security management areas. A software that automates the collection of event log data from security devices, such as firewalls, proxy servers, intrusion-detection systems, and antivirus software. The SIM (Security Information Management) translates the logged data into correlated and simplified formats

VI. ARCHITECTURE OF NETWORK SECURITY USING DES, AES AND RSA

Below figure showsthe simplification of this research paper.

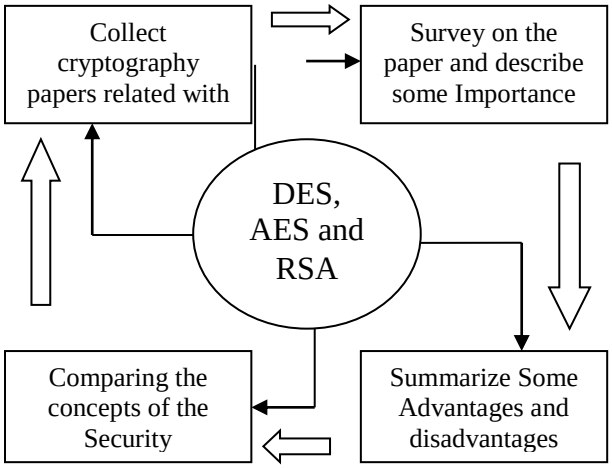

Fig 5: Architecture of Network Security using DES, AES and RSA

VII. Comparative Analysis Of DES, AES, and RSA

Among those applications they might have some equalize relation and also have some controversy. Some of them are listed below:

Table 1: Comparison between DES, AES and RSA

DES	AES	RSA
DES stands for Data Encryption Standard	AES stands for Advanced Encryption Standard	RSA acronym for Rivest, Adi Shamir
Key length is 56 bits	It uses various lengthsof the key Suchas 128, 192 and 256 bits	>1024 bits
It uses the Symmetric algorithm	It uses the Symmetric algorithm	It uses the Asymmetric algorithm
DES is developed in the year by 1977	AES is developed in the year by 2000	RSA is developed in the year by 1978
DES uses 6 rounds to encrypt and decrypt the text	AES uses 10/12/14 rounds to encrypt and decrypt the text	RSA uses 1 round to encrypt and decrypt the text
Encryption and Decryption process is moderate	Encryption and decryption process is faster	Encryption and Decryption process is slower
Security is not enough	It has excellent security	Low and poor security
Implementation of DES is, when compared with the software,hardware gives the better performance	It will become faster	Not as efficient or competent
Inherent vulnerabilities are Brute-Forced and Cryptanalysis Attack	For this Brute-Force attack only	RSA inherent vulnerabilities are Oracle and Brute-Forced attack

VIII. Conclusion And Future Enhancement

This paper presents a basic literature survey and comparing the work of few selected cryptography concepts and also presents security management areas for cloud computing. The selected crypt theories are DES, AES and RSA. Severaldifferences have been presented in this paper. Through this survey, till now DES performance ispoor and the process is always slow when comparing to another cryptography algorithm and which is having low security. This is the biggest drawback.

In our future work we find some drawback like key problem, file generation error, attacks, etc.and also simply the problem by the use of cryptographyalgorithms to solve thatproblem.

REFERENCES

[1] Dr.C.Priya et al.,**"Trusted Cloud Computing Platform in IaaS for Closed Box Execution Environment to VM"** in Journal of Advanced Research in Dynamical and Control Systems, volume 10, issue 4, 193-98, 2018, ISSN 1943-023X, SNIP 0.294, UGC Journal No. 26301

[2] R.Ranjani and Dr.C.Priya, **"A Fusion of Image Processing and Neural Networks for Lung Cancer Detection Using SVM In Matlab"** in International Journal of Pure and Applied Mathematics, Volume 119, issue 10, 100-111, ISSN 1311-8080(Print), ISSN 1314-3395(Online) 2018 Impact Factor: 7.19, UGC Journal No. 23425

[3] Prachi V. Bhalerao, et al., "Hardware Implementation of Cryptosystem by AES Algorithm Using FPGA", in IJCMC, Vol. 6, issue 5, pp. 84-89, May 2017.

[4] GurupinderKaur, Dr.Amandeep Singh Sappal. "Implementation of AES Algorithm on FPGA For Low Area Consumption", in International Journal of Advanced Research in Computer Science, Volume 8, No.7, pp. 704-707, July-August 2017.

[5] R.Ranjani and Dr.C.Priya, **"A Survey on Face Recognition Techniques: A Review"** in International Journal of Pure and Applied Mathematics, volume 118, issue 5, 253-74, ISSN 1311-8080(Print), ISSN 1314-3395(Online) 2017 Impact Factor: 7.19, UGC Journal No. 23425

[6] Dr.C.Priya,**"TaaS: Trust Management Model for Cloud-Based on QoS"** in Journal of Advanced Research in Dynamical and Control Systems, volume 9, issue 18, 1336-45, 2017, ISSN 1943-023X, SNIP 0.294, UGC Journal No. 26301

[7] Parson Raghav, et al., "Securing Data in Cloud Using AES Algorithm", in International Journal of Engineering Science and Computing (IJESC), Volume 6, Issue No.4, pp.3672-3675, April 2016

[8] Afolabi, A.O. &Atanda, O.G., "Comparative Analysis of Some Selected Cryptographic Algorithms", in Computing, Information Systems, Development Informatics & Allied Research Journal, Vol. 7, No.2, June-2016.

[9] C.Priya and Dr.R.Latha,**"TaaS: A Framework for Trust Management in Cloud Computing Environments"** in International Journal of Science and Research, volume 5, issue 9, 1402-05, ISSN 2319-7064(Online), DOI: 10.21275/ART20161879, September 2016.

[10] ShrutiSrivastava, A.Y.Kazi, "Design of AES on FPGA Hardware", in International Journal of Industrial Electronics and Electronical Engineering, Volume-4, Issue 9, pp. 152-154, Sep 2016.

[11] Ch.J.L.Padmaja, et al., "RSA Encryption Using Three Mersenine Primes", in Int.J.ChemSci, pp. 2273-2278, 2016.

[12] Ashraf Odeh, et al., "A Performance Evaluation Of Common Encryption Techniques With Secure Watermark System (Sws), in International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, pp. 32-38, May 2015.

[13] IsratJahan, et al., " Improved RSA cryptosystem based on the study of number theory and public key cryptosystem, in American Journal of Engineering Research, pp. 143-149, 2015.

[14] C.Priya and Dr.N.Prabakaran, **"A Research on Trusted Computing with Secure Resources for Multiple Clouds using Data Coloring"** in International Journal of Innovative Research in Computer and Communication Engineering, volume 3, issue 4, 3654-62, ISSN 2320-9801(Online),ISSN 2320-9798(Print), April 2015. Impact Factor: 4.447

[15] San San Tint, "Survey On Asymmetric Algorithm Using RSA Different Modified Models", in Computer Applications: An International Journal (CAIJ), Vol.1, pp.27-35, November 2014.

[16] Dr.PrernaMaharajan&AbhishekSachdeva, "A Study Of Encryption Algorithms AES, DES and RSA for Security", in Global Journal of Computer Science and Technology, Volume 13, Issue 15, 2013.

[17] C.Priya and Dr.N.Prabakaran**"A Research on Security prospects for Adopting Multiple Clouds through Cloud Computing"** in International Journal of Engineering Development and Research, volume 1, issue 2, 37-43,ISSN 2321-9939(Online), Sep-Oct 2013. Impact Factor: 1.79

[18] C.Priya and Dr.N.Prabakaran**"Security Management in Inter-Cloud"** in International Journal of Emerging Trends and Technology in Computer Science, volume 1, issue 3, 233-235,ISSN 2278-6856(Online), Sep-Oct 2012. Impact Factor: 4.413

[19] C.Priyaetal.,**"A Trust, Privacy and Security Infrastructure for the Inter-Cloud"** in International Journal of Computer Technology and Applications, volume 3, issue 2, 691-695, 2012, 2229-6093, March 2012.

[20] C.Priya et al., **"The Next Generation of Cloud Computing on Information Technology"** in International Journal of Computer Science and Information Technologies, Volume 2, No 5, 2011, ISSN 0975-9646.

[21] C.Priya et al., "**Monitoring System using Smart Phones**" in International Journal of Computer Engineering and Technology (IJCET), Jan 2011Vol. 1(3), 2011, 0976-6375.

[22] M.Kannan and Dr.C.Priya, **"A survey on fault detection enabled Optimal Load Balancing Technique by efficient utilization of VM in Cloud Computing"** International Conference on Computing Sciences (ICCS), ISBN 978-81-910217-0-9, pp.84