

A Simulation Tool for Security of Hardware Resource Utilization Information in Cloud Environment with EnDeCloudReports Tool

Amita Sharma
Asst.Professor(CS)
IIS University, India

Shweta Singh
Ph.D. Scholar (CS)
IIS University, India

ABSTRACT

A cloud storage mechanism repressed a storage device design and cloud based protocols. Cloud storage architecture can be exposed design for remote method access through cloud storage device. Cloud storage is a centralized data distribution center meant for authorized clients, among them cloud data will share towards different clients as apiece their authority in addition to access permissions. Based on this assortment of researches are being proceeding. However, within this article it focuses the storing data in the midst of fully secure in cloud report also. The swift progression of the cloud has formed it as a desirable ambition of attack intended for both foreign attackers and malicious insiders. Files, blocks, data sets and objects are common logic units of data storage within cloud storage device mechanism. In this research it pioneer with a new set of methods or new unit of methods handled by means of the AES algorithm meant for creating strong encryption and decryption.

Keywords

Cloud Report, EnDeCloudReports, Secure Sockets Layer (SSL), Transport Layer Security (TLS), Certificate Signing Request (CSR), Certificate Authority (CA), Internet Engineering Task Force (IETF).

1. INTRODUCTION

Cryptography technology was in full swing from the beginning of the Second World War for transferring information with security. Subsequent to that, tons of the algorithms are derived for encrypt and decrypt the secured data. In this research paper, it fetches AES algorithm in order to keep data in the cloud service secured. Most imperative concern connected towards cloud storage is the security, integrity and confidentiality of data, which turn out to be more prone in the direction of being compromised, while, entrusted towards external cloud providers as well as other third parties. There can furthermore be legal and regulatory implication with the intention of results from relocating data across geographical or national boundaries. Additional issues apply explicitly towards the performance of a large database.

LANs provide locally stored data by means of network reliability and latency levels that are superior to those of WANs. Unfortunately, current cloud simulation tools similar to cloud reports (a GUI interface of cloud report tool) are not capable to aid researchers in securing the raw data files generated on behalf of presenting the cloud environment usage in pictorial form. This research article presents by EnDeCloudReports, cloud report based tool, which can encrypt/decrypt the raw data files generated, by cloud reports tool and are requisite meant for the development of graphical representation of resource utilization in cloud environment architectures being simulated by means of researchers.

Presume, attackers gained the control of a cloud system or managed to obtain the system information furthermore plan to perform a POST attack scenario. If able to get RAM info, Memory info, Data Center Server of the hardware, which is being stored in raw data form, intruders are able to take/grasp data in the flow of pointers/pointing access. If using different/innovative cryptography methods and encryption/decryption rounds, can be able to generate highly secured Cipher text used for storing data in the cloud.

1.1. Cloud Security Guidance

A prescriptive series of steps that has to be taken by cloud consumers to evaluate and manage the security of their cloud environment with the goal of mitigating risk and delivering an appropriate level of support. The following steps are to be followed discussed in detail:

- Ensure effective governance, risk & compliance processes exist
- Business processes & Audit operational
- Handle people, identities and roles
- Proper security measures for data security in cloud
- Enforce confidentiality policies
- Measure the security necessities for Cloud Report Tool based Applications
- Ensure cloud Networks (N/W) and Connections are safe
- Evaluate protection controls on physical utilities and infrastructure
- Manage protection scenarios in the cloud SLA

2. ANALYSIS FOR THE EnDeCloudReports

Encryption algorithm has very significant role in Communication security. The performance of existing encryption techniques like AES, DES and RSA algorithms was surveyed and analyzed on the basis of an experiment based on text files in terms of Packet size, Encryption time, and decryption time and concluded that the AES algorithm consumes least encryption time and RSA consume longest encryption time. It observed that Decryption through AES algorithm is better than other algorithms when compared on the basis following factors (Prerna Gupta, 2013):

1. Block size
2. Key size
3. Power consumption
4. Encryption time
5. Decryption time
6. Deposit keys (yes/No)
7. Security
8. Inherent Vulnerabilities
9. The Key used

10. Hardware and Software implementation
11. Ciphering and deciphering algorithm
12. Rounds
13. Trojan Horse
14. Simulation Speed

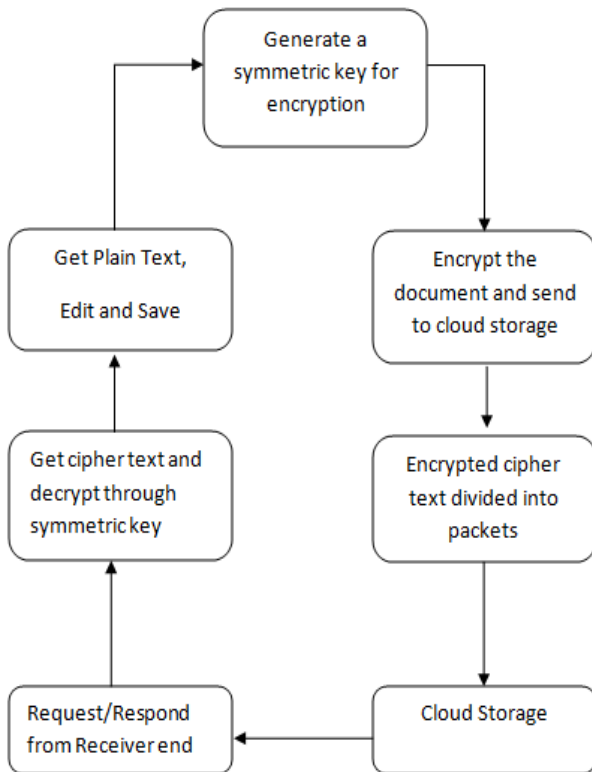


Figure1: Basic working structure of EnDeCloud Reports

From the simulation result, it evaluated that AES algorithm is much better than DES and RSA algorithms. In this study the file, CryptoUtils.java is holding the AES operation, and CryptoFileUtils.java is responsible for the file operation. Which is calling the CryptoUtils.java for the encryption/decryption key and ExceptionCrypto.java is handling the exceptions while execution of the code. Malware generally developed for illegal purposes, but can also be utilize for sabotage, usually without direct benefit to the perpetrators.

2.1. Secure Socket Layer

The SSL and TLS are the main as well as extensively arranged security protocol. It is fundamentally a protocol with the purpose of providing a secure channel linking two machines operating over the Internet or an intranet. SSL is a translucent protocol, which necessitates very small interaction starts the end user while determining a secure session. SSL protocol developed by Netscape intended for transmitting private documents throughout the Cloud Infrastructure (Internet). SSL uses a cryptographic system with the aim of using two keys towards encryption of data, a public key recognized towards each person as well as a private or secret key recognized merely to recipients of the message.

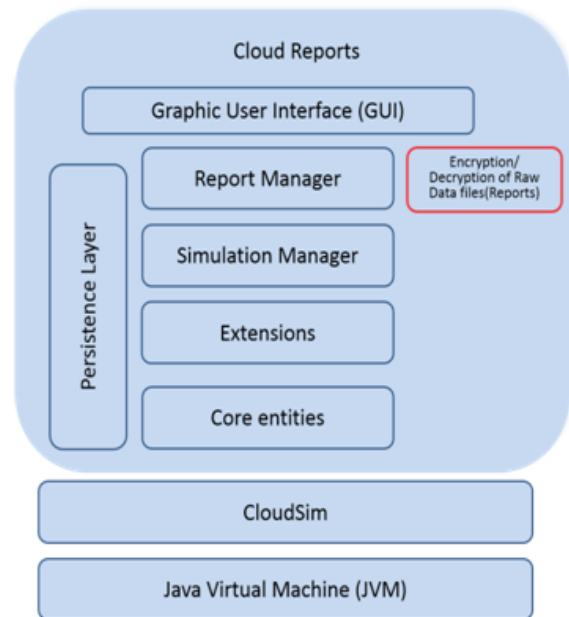


Figure2: Modular software architecture of EnDeCloudReports

2.2. HTTP and SHTTP

In order to secure the connections over an email client such as Microsoft Outlook and an email server such as Microsoft Exchange for securing the transfer of files over HTTP, SHTTP and FTP services for instance website editing authorized members transferring large files through SSL is required. SSL is a standard security technology for establishing an encrypted link between a server and a client characteristically a web server along with a browser. Protocols explains how algorithms ought to be used, in this instance the SSL protocol includes the variables of the encryption for connecting both the client as well as the server and the data is transmitted by implementing the AES algorithm.

Properties of Data packets:

- The source IP address
- The destination IP address
- The sequence number of the packets
- The type of service
- Flags
- Etc

2.3. SECURE HTTP (sHTTP)

The HTTP protocol to sustain sending data secure in excess of the WWW. The entire servers and web browsers do not support SHTTP. SSL is an additional widespread for secure transaction. Whereas SSL is designed in order to ascertain a secure connection between two computers, S-HTTP is a secured design, to send individual messages securely. Together protocols encompass begin submitted are headed for the IETF on behalf of approval as it is a standard being followed. An additional protocol for transmitting data securely above the WWW is sHTTP. While SSL creates a secure connection between the client and the server, over which different and huge chunks of data sent securely, sHTTP is premeditated in order to transmit individual messages securely. SSL and sHTTP, as a result, which will be able to observe as complementary relative than competing technologies. The IETF as a standard approved in favour of both the protocols.

The Servers and the clients speak precisely over the similar HTTP towards each other, however, over a secure SSL connection with the intention of encryption along with decryption of the respective requests and responses. The two main purposes of SSL layer:

- Authentication with the respect to communicate directly with the server
- Certify the server to read what the user sends and read what the server sends back to the user

2.4. SSL Certificate and its Work

A couple of key set work simultaneously to set up encrypt and decrypt connection:

1. Making CSR in the server
2. CSR makes a private key as well as public key within the server
3. The CSR data file to dispatch in the direction of the SSL Certificate issuer (CA) encloses the public key. The CA utilizes the CSR data file in order to make a data structure towards match private key without compromising the key itself. The CA under no circumstances perceive private key

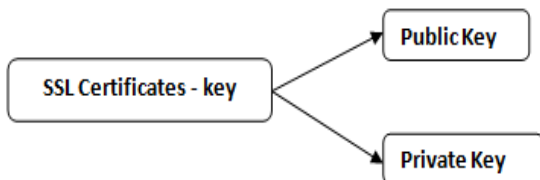


Figure3: SSL Certificates – Key Pair

Browsers approach by means of a pre-installed list of reliable CAs, recognized as the Trusted Root CA store. An SSL Certificate issued by a CA headed for an organization as well as its domain/website ensures that a trusted third party has authenticated that organization's uniqueness. In view of the fact that the browser trusts the CA, the browser at present trusts that organization's identity. The browser allows the user to be acquainted with the fact that the website is secure and the user experiences safe and secure while browsing the website along with entering their confidential information.

2.5. GENERATE SSL Certificate's - SECURE CONNECTION

While a browser attempts to access a website securely one through SSL, browser and web server establish an SSL connection by a procedure called SSL-Handshake.

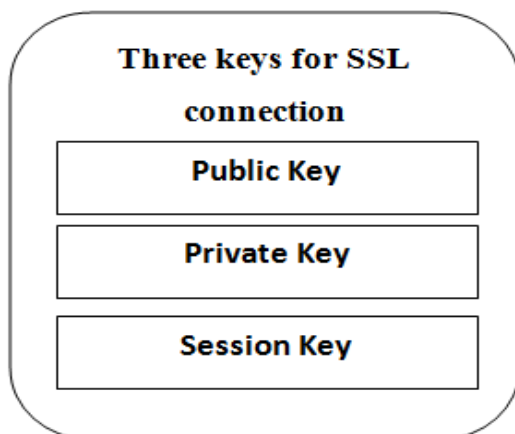


Figure4: Key set for SSL Connection

Encrypting as well as Decrypting amid private and public key obtains a group of processing power, those used inside throughout the SSL-Handshake towards creating a symmetric-session key. Subsequently, after generating a secure connection, the session key has used to encrypt the entire transmitted data.

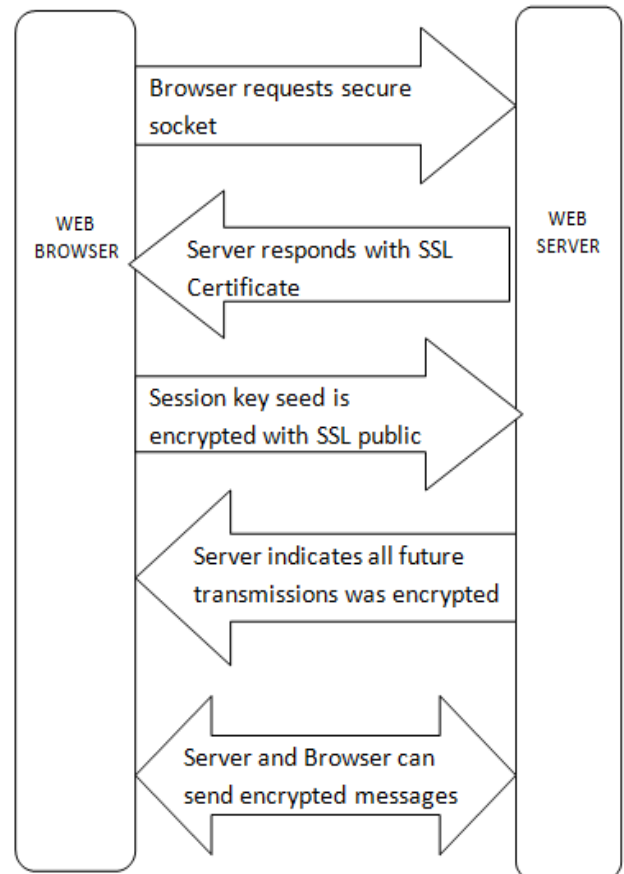


Figure5: SSL Establishing Connection

2.6. ESTABLISHED SSL CONNECTION

An SSL connection between a client and server has positioned by a handshake, the aim of the SSL handshake is:

- Towards gratifies the client with the intention of it is talking en-route to the right server
- Meant for the parties towards having an agreed on "cipher suite", which comprise which encryption algorithm they determination utilize towards exchange data
- On behalf of the parties towards having an agreed on whichever necessary keys for this algorithm

2.7. Certificate Exchange

At the instance when the connection is established, the server is required to show its individuality towards the client. This has acquired through its SSL certificate, which has a very little bit similar to be known as its passport. SSL certificate encloses various pieces of data, along with the name of the owner, the property; it has attached to, the certificate's public key, the digital signature as well as information in relation to the certificate validity dates. The trustees verifies that implicit beliefs the certificates or it was verified plus trusted with one of several CAs with the intention of it too implicitly trusts.

2.8. Key Exchange

Symmetric algorithm uses a single key meant for encryption as well as decryption, in contrast towards asymmetric algorithms where a public/private key pair is required. Both parties require the concurring on this single, symmetric key, a process with the aim of is accomplished securely using asymmetric encryption plus the server's public/private keys.

3. RECEIVER MACHINE: PACKETS AND ARRANGING

When a node has multiple packets to send during a sending slot, it can increase its own duty cycle and request other nodes beside the route to the sink to do the same. This implemented through a slot-by-slot renewal mechanism using a data flag in the MAC header. A receiver checks for this flag and if set, it returns an acknowledgement that has more data flag set. It then stays awake to receive and forward one additional packet.

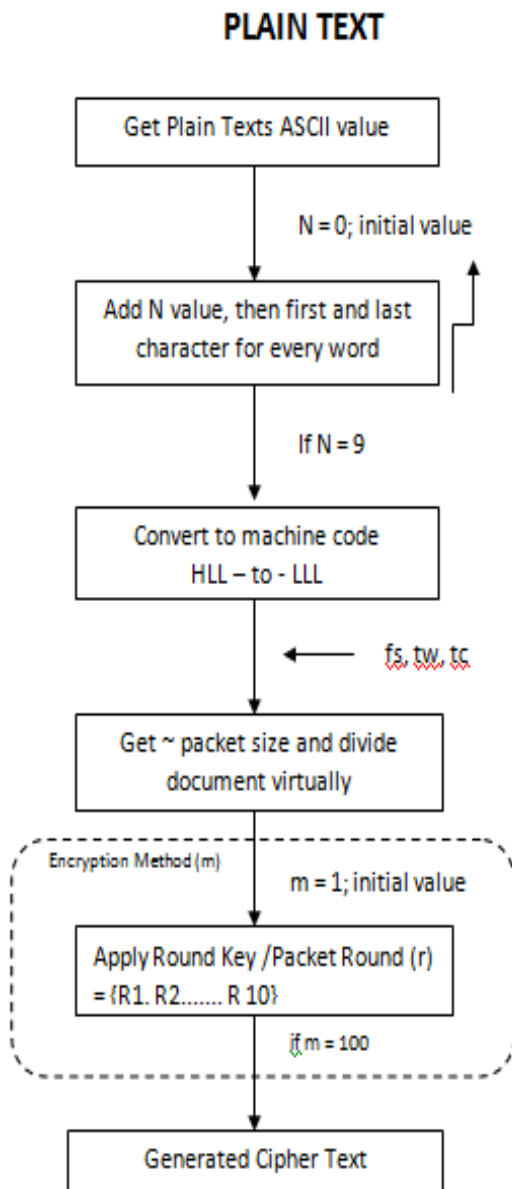


Figure6: Encryption-Plain text to cipher text

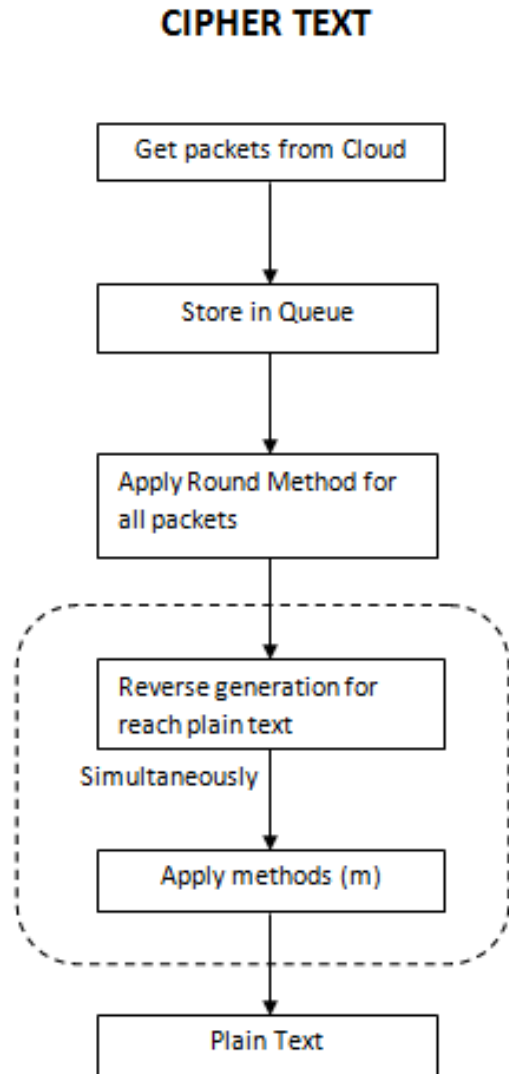


Figure7: Decryption- cipher text to Plain text

3.1. Digital Signatures

SSL documentations encompass a linked public/private key pair. The public key had dispersed as part of the documentation, along with the private key, which is reserved and extremely safeguarded. This pair of asymmetric keys used within the SSL handshake in the direction of exchange a further key intended for both parties in order to symmetrically encrypt and decrypt data. The client utilizes the server's public key towards encrypt the symmetric key as well as send it securely en-route intended for the server, and the server uses its private key towards decrypt it. Everyone is able to encrypt by means of the public key, other than merely the server is capable of decrypting with the private key.

The conflicting is factual intended for a digital signature. A certificate will be able to be "signed" with another authority, In this case, the authority makes use of their private key to encrypt the contents of the certificate, in addition to this, the cipher text is attached to the certificate as its digital signature. Everyone is able to decrypt this signature by means of the authority's public key, furthermore to confirm that it results within the expected decrypted value. Merely the authority can encrypt the content with the private key, moreover, authority only can actually create a valid signature in the first place.

3.2. Round Methods with AES Algorithm

AES Algorithm

AES is an iterated symmetric block cipher,

- AES works by repeating the same steps (Multiple times)
- AES - secret key Encryption Algorithm
- AES operates a scheduled fixed number of byte(s)

AES is a symmetric block cipher. That means that a similar key has used to encrypt and decrypt data. A number of AES parameters depend on the key length. For example, if the key size used is 128 bits, then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively.

Normally, if an encryption technique has used for sending a document, at first an encryption algorithm executes first to generate cipher text. Followed by encryption the document has sent from a source machine to the receiver or client to server or from a network area /cloud (private/public/hybrid) to the cloud. In this, 100 methods have been used in rounding/rotating.

Encryption and Decryption Method = m

Set (m) = {m1, m2, m3.....m100}, r → Rounds
 F(r) = {r=1; r++; r>=10}
 if r = 10; then r = 1; return;

For Sample: 44bytes / Packet
 1024 KB = 1 MB
 44 Bytes = 1 Packet
 1024/44 = 23 packet and 12 bytes
 12 bytes + 32 dummy bytes = 24 packet,
 1st packet have 44 bytes,

Packet → P
 Set (P) → {Pi1, Pi2, Pi3,, Pin}
 Base (n) = total number of packets
 Pin = n-th Packet id
 Loop for using AES algorithm
 Loop starts from 0 to 9
 N → single word's id

f(s) = {N=0, N++,N>= 9}
 if N = 9 then N Initial value (0)
 START LOOP
 {
 Segregate words in giving document file,
 1st word => last char N(0) word 1 N(0) first char
 2nd word => last char N(1) word N(1) first char
 10th word => last char N(9) word 10 N(9) first char
 “ “ “
 “ “ “
 “ “ “
 Nth word => last char N(n) word(n) N(n) first char
 }
 Check N(n), if n = 9,
 End Loop;
 N = 0,

Start word count from last loop
 If there are no words to insert into the loop, end the loop,
 After N(n) → Convert to Binary value (Based on word count N value will differ), Start is swapping in Binary values,

Swap the bytes for generating encrypt word → BOOK
 B O O K
 10000100 10011110 10011110 10010110

K0BOOK0B → AES (Plain Text with AES form)

1001 000 1000 1001 1001 1001 0000 1000
 0110 000 0100 1110 1110 0110 0000 0100
K 0 B O O K 0 B

Below table concentrates for a single character or a byte

| | | |
|--|------------------------|---|
| 2 bytes (Last character, N-word(s) id) | A – character (1 Byte) | 2 bytes (N-word(s) id, First character) |
| 8-bits + 8-bits | 8-bits | 8-bits + 8-bits |

Need to concentrate on word length it may be a single letter word or multiple char word. After applying the AES algorithm model files size increases. Therefore, in the time of dividing documents into packets itself, it considers taking three reports, the total number of word count, number of characters (alphabets, numeric values and special characters) and file size in bytes.

File size in bytes = fs;
 Total number of words = tw;
 Total number of characters = tc;

Generate array:

Array[] = 1D array;
 Each space considers and occupies five – bytes;
 Array → each array is a packet

Array → Array a1[];

When the option for pre-fixing the packet size of the application is set, as per the selected user to declare the array formation and size, according to that array count will increase and fix constantly based on the file size.

a1 [] = {a1[0], a2[1],.....a44[43]}
 P1 (EOF - id) = (a1 [a44]+1)
 a2 [P1 (EOF-id)] = {a2 [45], a2 [46], a2 [47],a2 [89]}
 “ “ “

Pn → (n) Total packet count

Based on document size, array count and packet count will increase.

Implementation of Set (m) = {m1, m2, m3.....m100}

| | | | | |
|----------|----------|----------|----------|----------|
| 10000010 | 00000000 | 10000010 | 00000000 | 10000010 |
| A | 0 | A | 0 | A |

Start from 0th to 17th, 1st to 18th, 99th bit = m (100th step)
 0th bit to 8th bit
 1st bit to 16th bit
 2nd bit to 17th bit
 3rd bit to 18th bit
 4th bit to 19th bit

Count (bytes) → get last byte (lb)
 lb to lb1 - 8 bit (lb2)
 lb2 - 8th bit (lb3) to lb3 - 15 bit (lb4)
 lb3 to lb3-15 bits (lb4)
 lb4 to lb4-15 bits (lb5)
 lb5 to lb5-15 bits (lb6)

3.3. SSL/TLS Encryption: Challenge in Cloud

SSL more properly called TLS, has become the default approach for protecting sensitive data flowing over the Cloud. SSL uses encryption to present data confidentiality for connections between users and websites and the cloud based services they provide. The growth in the use of web applications and cloud based services and even the need to encrypt internal networks is driving a quick increase in the number of SSL connections and a matching population of SSL related keys and certificates. The operational challenges of managing this expansion can outshine vital security consideration.

Table 1. Experiment results of Derived AES Algorithm.

| S. No | Packet Size | Encryption Time(ms) | Decryption Time(ms) |
|-------|-------------|---------------------|---------------------|
| 1. | 165 | 1.2 | 0.8 |
| 2 | 225 | 1.5 | 1.3 |
| 3. | 375 | 1.9 | 1.4 |
| 4. | 925 | 2.5 | 1.7 |

4. CASE STUDY

Environments for simulation created using CloudReports are involved of provider in the infrastructure as a service (IaaS) and an arbitrary amount of users in the cloud. Provider of IaaS would have one or more centres for data, each of one are modelled characteristics independently like allocation policies of virtual machines, costs for operation and utilization of resource thresholds. It is probable for configuring every center for data host individually. Users in the cloud are modeled as a virtual machines set for allocated by the infrastructure which is managed by profile for utilization and provider of IaaS. Each and every virtual machine has to be configured using particular characteristics like central processing unit, hypervisor type, memory demand and Cloudlet Scheduler. Profile for utilization identifies how Cloudlets would behave with respect to utilization of resource once they are executed. The Cloud Environment built up for the case study is shown in figure 7

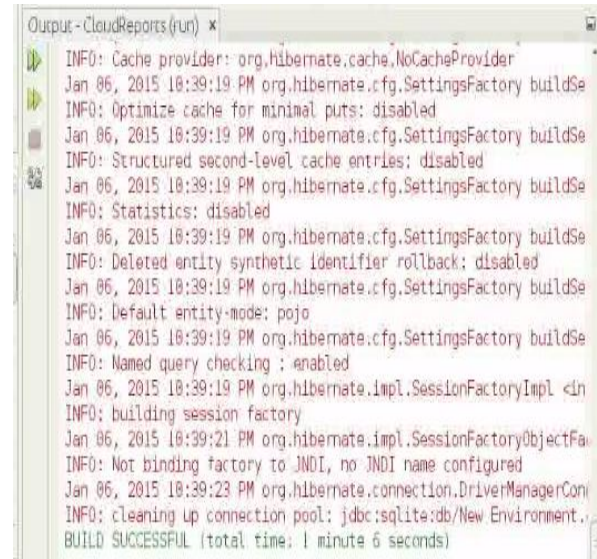


Figure 7. Building the CloudReports Environment

As modelling for workload plays a decisive role based on the simulation experiments outcomes, it is needed for using a model which is as same as probable to real environments of data center. Thus, in this case study, experiments made use of information gathered from the data project of Google Cluster is publicly available from set of utilization for resource are identified from real cluster are managed by Google with nearly 12,000 machines.

Workload applied to environments that are simulated is modeled in CloudSim are denoted by class of Cloudlet are allocated in hosts are executed on virtual machines. Traces obtained from data of Google Cluster have data relative to use of resources for example memory, central processing unit and disk and are represented as jobs which execute on real machines from monitored cluster. For using these traces on experiments for simulation, data from the jobs was denoted as Cloudlets. Experiments adopt traces of consumption of power gathered from real machines benchmarks that is available by corporation of standard performance evaluation. Four various virtual machine policies for allocation are adopted in the experiments. Such policies determine how node in the controller has to distribute virtual machines among all presented hosts.

Single static threshold policy has a single threshold for utilization that identifies if a host is overloaded. Median absolute deviation-MMT (Minimum migration time) policy has dynamic thresholds for utilization and was obtained (Beloglazov and Buyya, 2012). Double static threshold policy has two thresholds for utilization. 1st identifies if a host is overloaded and 2nd is adopted for identifying under-used hosts. Local regression-MMT policy has dynamic thresholds for utilization like previous policy was obtained from Beloglazov and Buyya, 2012

Regarding the configuration of virtual machines, experiments adopted 4 profiles type on the basis of services from real provider of infrastructure as a service. Text file generated for this case study before encryption is shown in figure 8.

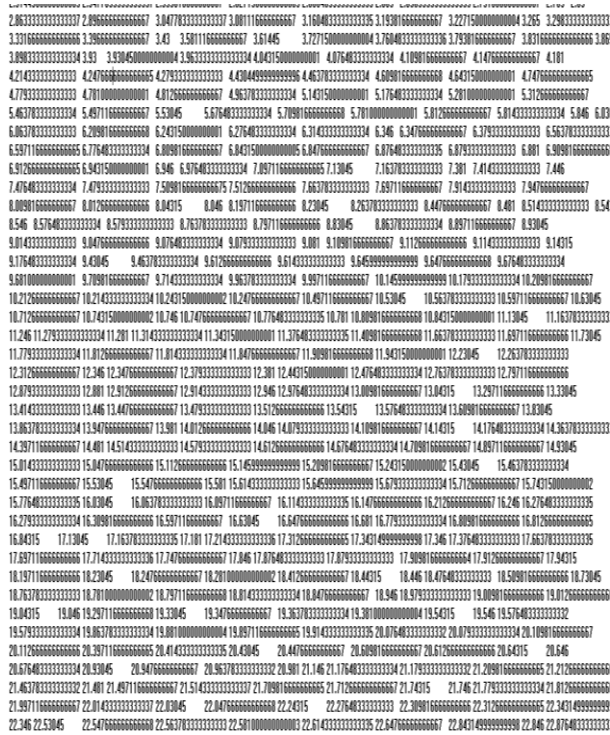


Figure 8 Text File before encryption in EnDeCloudReports

File after encryption through derived AES algorithm is shown in Fig. 9



Figure 9 Encrypted File in EnDeCloudReports after implementing derived AES Algorithm

5. CONCLUSION

Security is one of the biggest challenges in the cloud. Anyone can access the cloud data from their own end. There is no mechanism to control data access. Sharing is the direct access of data from the storage area. Assortments of mechanisms have generated for predicting the data from intruders by using many cryptography algorithms. Intruders can attack cloud directly or at the time of sending data from the client to the cloud or receiving from the cloud to the client. Since these, all have occurred between TLS and SSL. Use to give protection in all three parts. Therefore, at the time of generating file take steps for security simultaneously. In this paper, new methods have implemented in the AES algorithm with a set of

methods. Encryption and decryption conversion code will be available in the application. In the private access, cloud data takes the concept as an important role in keeping data in secure. The IT department must log security events for all critical systems. The proposed model provides compelling methods, since the obtained results of the experiments are close to the model output using the real-data sets. To implement new encryption and decryption technique for overcoming the hackers and intruders knowledge to give protect to the cloud storage data and in transaction layers. Our research model of EnDeCloudReports and derived AES algorithm can extend to various web-based applications (such as e-commerce etc.).

6. FUTURE SCOPE

In future we will compare the experiment results of derived AES algorithm shown in this paper with other existing cryptography algorithms for encryption and decryption of text files in Cloud Environment.

7. REFERENCES

- [1] Aparjita Sidhu and Rajiv Mahajan, Enhancing security in cloud computing structure by hybrid encryption, International Journal of Recent Scientific Research Vol. 5, Issue, 1, pp.128-132, January, 2014.
- [2] Chou, Te-Shun. "Security Threats On Cloud Computing Vulnerabilities." International Journal of Computer Science & Information Technology (IJCSIT) Vol 5 (2013).
- [3] Dr. Prerna Gupta & Abhishek Sachdeva IITM India (Eds)-A Study of Encryption Algorithms AES, DES and RSA for Security. (Global Journal Inc.) Volume13 Issue 15. Year 2013.
- [4] Khan, Miss Shakeeba S. , and Miss Sakshi S. Deshmukh. "Security in Cloud Computing Using Cryptographic Algorithms" (2014).
- [5] Liu, Wentao. "Research on cloud computing security problem and strategy". Consumer Electronics, Communications and Networks [CECNet], 2012 2nd International Conference on. IEEE, 2012.
- [6] Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy. "Cloud Computing: Security Issues and Research Challenges", International Journal of Computer Science and Information Technology & Security, 2011.
- [7] Swati Kashyap, Er. Neeraj Madan, Haryana Engineering College, Network Security and Cryptographic Algorithm, ijarscs journal, Volume 5, Issue 4, April 2015.
- [8] E. Cole, R. Krutz and J. W. Conley, Network Security Bible, Wiley Publishing Inc, 2005.
- [9] A. Menezes, V. Oorschot and A. Vanstone, Handbook on Applied Cryptography, CRC Press Inc., NY, USA, 2000.
- [10] D. Stinson, Cryptography Theory and Practice, CRC Press Inc., NY, USA, 1995.
- [11] G. Blelloch, Introduction to Cryptography, online: <http://www-2.cs.cmu.edu/afs/cs/project/pscico-guyb/realworld/crypto.ps>, 2000, accessed on Sept. 1, 2008.

- [12] G. Carter, E. Dawson and L. Nielsen, Key Schedule Classification of the AES Candidates, in Proceedings of the end AES Conference, Rome, Italy, 1999.
- [13] J. Dray, Report on the NIST Java AES Candidate Algorithm Analysis, online: <http://csrc.nist.gov/encryption/aes/round/r1-java.pdf>, 1999, accessed on Sept. 1, 2008.
- [14] J. Dray, NIST Performance Analysis of the Field Round Java AES Candidates, online: <http://csrc.nist.gov/encryption/aes/round2/conf2/papers/8-jdray.pdf>, 2000, accessed on Sept. 1, 2008.
- [15] J. Nakahara, B. Preneel and J. Vandewalle, Square Attack on Extended Rijndael Block Cipher, COSIC Technology Report, 2002.
- [16] D. Baudran, H. Gilbert, L. Granboulan, H. Handschun, A. Joux, P. Nguyen, F. Noilhan, O. Poincheva, T. Pornin, G. Poupard, J. Stern and S. Vaudenay, Report on the AES Candidates, in Proceedings of the 2nd ASE Conference, Rome, Italy, 1999.
- [17] T. Verhoeff, Cryptography, online: <http://www.pa.win.tue.nl/wstomv/software/AESRijndael/rijndael-test.pas>, 2001, accessed on Sept. 1, 2008.
- [18] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3rd ed., Prentice-Hall, 2003.
- [19] W. Stallings, Cryptography and Network Security, 4th ed., Prentice-Hall, 2005
- [20] B. A. Forouzan, Data Communications and Networking, 4th ed., McGraw-Hill, 2007
- [21] Wikipedia Website, online: <http://en.wikipedia.org>, accessed on Nov., 13, 2008.