AES AND DES Technique Used in Cloud Computing Environment

Prachi Garg[1], Dr Sandeep Goel [2], Saurabh Garg[3]
Research Scholar [1]
Professor[2]
Research Scholar[3]
Computer Department
M. M. Engineering College,
Maharishi Markandeshwar University

Abstract: The objective of the study is to inspect the safety restriction and highlight the present dangers in cloud computing real safety procedures for cloud computing systems. It will assist the researchers to categorize security provisions at several stages to recognize the threats in the numerous cloud computing models modeled by mutually interior and exterior customers. Thus, it will beneficial to explain cloud security protocols that guarantee the safety of the cloud environment. In this paper we work AES and DES Based approach using Cloud Computing. Evaluate AES and DES encryption and Decryption timing

Keywords: Cloud Computing, AES,DES,SHA,ECC

I. INTRODUCTION

Nowadays a portion of persons are referring their mail online over webmail patrons, inscription cooperative leaflets by means of web browsers, making virtual folders to upload their photographs of the trips[2]. They are consecutively requests and stowage information in servers situated in internet and not in their individual processors. Somewhat as modest as arrive in a web page is the solitary object a consumer wants to start to custom facilities that exist in on a distant server and leases him share isolated and private info, or by means of computing series of a mound of servers that he will always understand with his personal eyes and each day its being used additional to these facilities]8] that are named cloud computer facilities. That term is assumed since of the symbol around Internet, as rather than the consumer understand similar to a cloud and cannot understand what's private. These facilities can be obtained by permitted or by disbursing by request (pay for consume), can be merely similar to a purpose calling (like requesting the temperature in some city in the world for comprising it in a web page) or compound (similar to the practice of a virtual machine with its personal operating system, applications and stowage space for running applications). This means that numerous consumers and groups can evade connection to the requests in their computer or can have additional computational control by means of cloud computer over internet, or they can create their individual secluded cloud to achieve it totally, or they can usage both choices for the instants of extraordinary request of consumption.

Cloud computing is a novel and developing expertise where practical infrastructure is delivered by way of "service". In this method, customers of clouds (software designers) can custom virtualized resources as a facility, frequently compliantly scrabbling resource custom (and expense) up or down. One of this computing technology provision layers, Infrastructure-as-a Service (IaaS), provides[16] designers liberty to advance their individual policy and custom their software by way of they would fix on their personal infrastructure, then this arises with a cost: handling software structural design on a large cloud at runtime can be a tough and subtle job, by way of individual minor mistake in a utilization script or an architectural alteration can consequence in thoughtful responsibilities ensuing in renunciation of facility or supplementary severe disappointments as a importance.

II.CLOUD MALWARE – INJECTION ATTACK

This one is the earliest substantial outbreak effort that inserts application of a malevolent facility or virtual machine into the cloud. The resolution of threated cloud is everything that the challenger is attentive in, it might contain information alterations, complete functionality variations/contrary or overcrowdings. In this outbreak[18] challenger generates its individual malevolent facility operation component (SaaS or PaaS) or virtual machine example (IaaS), and enhance it towards the cloud system. Formerly, the challenger has to fictitious to the cloud organization that it is approximately the novel facility application example and amongst the legal examples for nearly specific facility criticized by the challenger. Uncertainty this achievement prospers, the cloud mechanically sends the requirements of lawful customer to the malevolent facility operation, and the challenger's cipher is implemented. The chief situation behindhand the Cloud Malware Injection attack is that assailants transmit an influenced/incorrect duplicate of a wounded facility example thus malevolent example can attain admission to the facility needs of the target's provision. To attain this, the assailant has to originate regulator finished the wounded information in the cloud. Allowing to arrangement, this outbreak is the main illustrative of abusing the service-to-cloud outbreak superficial.

2.1 Malware-Injection Attack Resolution

1. Usually, once a client unlocks an account[1] in the cloud, a copy of the consumers VM in the duplicate source scheme of the cloud is delivered through the supplier. The requests track through the client is reflected by great competence and

reliability. Deliberation of the reliability in the hardware level must stay keen on account, since it is very hard for an assailant to interrupt at the IaaS level. File Allocation Table (FAT) scheme design is used, meanwhile its forthright method is reinforced through entirely present virtual operating systems. Since the FAT table info around the cipher or request that a client is accepted to track can be raised. Squared completed the preceding examples that had been previously performed after the client's mechanism can be placed to control the legitimacy and honesty of the novel example. On behalf of this determination, a Hypervisor at the suppliers end, essential to be positioned. This Hypervisor will be well-thought-out the greatest protected and refined portion of the cloud scheme whose safety cannot be penetrated through at all means. The Hypervisor is accountable for arrangement of the entire occurrence facilities, nonetheless earlier arrangement it will check the reliability of the example commencing the FAT table of the consumers VM.

2. Additional method is to accumulate[11] the operating system kind of the client in the primary stage after a consumer unlocks an account. Since the cloud is completely operating system platform liberated, beforehand initiation an example in the cloud, irritated examination can be completed through the operating system kind after which the example was demanded after through the account owner operating system kind.

2.2 Authentication Attack

Validation is a feeble matter in the introduced and virtual facilities and is very repeatedly beleaguered. Here are accordingly numerous methods to validate operators that can be founded upon whatever a consumer identifies, needs, or remains. The mechanisms and the approaches that are applied to protect the verification procedure are typically beleaguered through the assailants. Lately, concerning the structural design of cloud computing, SaaS, IaaS and PaaS,[12] here is individual IaaS that is capable to compromise this type of info guard and information encoding. Uncertainly the conveyed info concealment is below the grouping extraordinary for some innovativeness, the cloud computing facility founded on IaaS design will remain the greatest appropriate and conceivable answer for protected information message. In adding, the approval of information procedure or organization for that information fitted to the initiatives but deposited on the facility supplier's lateral must be official through the consumer side (enterprises) to in its place of the facility suppliers.

2.3 Authentication Attack Resolution

Maximum user-facing facilities nowa[9]days static usage modest username and password kind of knowledge-based verification, through the exemption of approximately economic organizations that must organized numerous procedures of subordinate verification (such as site solutions, virtual keyboards, common secret queries, etc.) to create it a bit additional problematic for general phishing outbreaks.

III. RELATED WORK

The security challenges [21] for cloud computing approach are somewhat dynamic and vast security challenges [21] . cloud computing security Data location is a crucial factor. cloud computing Location transparency is one of the prominent flexibilities, without knowing the specific location which is a security threat at the same time of data storage, the provision of data protection act for some region might be severely affected and violated. cloud computing environment Cloud users' personal data security is thus a crucial concern. These slides [22] tell us about security that it gracefully loses control while maintaining accountability even if operational responsibility falls upon 3rd parties. Also it tells us that the Provider and user security duties differ greatly between cloud models.This paper gives the 7 different security issues [23]. Author [24] proposes a cloud environment by enabling using a Trusted Third Party within trust and using cryptography to ensure the confidentiality, integrity and authenticity of data and communications, while attempting to address specific security vulnerabilities. expresses the customer's faith in specific operational, notion of trust against a Third Party, ethical and quality characteristics, while it also includes the acknowledgement of a mini-mum risk factor. The aim of [25] firstly to attempt to present aviable solution that eliminates these potential threats and evaluate cloud security by identifying unique Security requirements. proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed specifically Public Key Infrastructure operating in concert with SSO solution calls upon cryptography, and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communication

IV. PROPOSED SYSTEM

4.1 AES Based approach using Cloud Computing

Here, our goal is to measure the Encryption and Decryption speed of each algorithm for different packet sizes. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased. By considering different sizes of data blocks (0.5MB to 20MB) the algorithms were evaluated in terms of the time required to encrypt and decrypt the data block. All the implementations were exact to make sure that the results will be relatively fair and accurate.

V. RESULTS ANALYSIS

The proposed approach has many modules. The first and the most important upload a file on cloud Data. Next module is based on encryption and decryption algorithms i.e. AES and ACC Java 1.7, Apache Tomcat Server and Box.com for cloud have been used for implementing the proposed approach. The proposed system provides better security as compare to previous authors. Front end of the project shows the following options like Home, Login, Signup, Upload File, Download File, about us and Sign out. If the user is not register they has to first their own self than they can upload or download the file on cloud with secret key Fig. shows the uploading of an image file on cloud with the secret key. We have obtained a modest execution of a convenience that produces hash of the document. The instrument castoff for this application is Netbeans IDE and the programming linguistic used is Java. The hash purpose used to produce hash value in this request is SHA. Procedure through advanced safety alike SHA can be castoff if desirable. In circumstance once illegal being creates the variations to the content of the document it unavoidably variations too the honesty and the hash value of the document as well. In this circumstance when we associate the hash values of the document we can realize that hash has altered as offered in the figure.

The Simulation program (shown in Fig) accepts three inputs: Algorithm, Cipher Mode and data block size. After a successful execution, the data generated, encrypted and decrypted are shown. Another comparison is made after the successful encryption/decryption process to make sure that all the data are processed in the right way by comparing the generated data (the original data blocks) and the decrypted data block generated from the process.

The following tasks that will be performed are shown as follows: - A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time at two different encoding bases namely; hexadecimal base encoding and in base 64 encoding. - A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm. -A study is performed on the effect of changing data types -such as text or document and images- for each cryptography selected algorithm on power consumption. - A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

The popular secret key algorithms including DES, 3DES, AES, Blowfish, were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in a uniform language (Java), using their standard specifications, and were tested on two different hardware platforms, to compare their performance.

The encryption simulation was performed on DES, AES and Blowfish algorithms had been carried on NetBeans IDE 7.4.The encryption simulation is probably the most fundamental type of cryptographic analysis that can be performed on the algorithms under study. This simulation is simple and standardized. In this work, the 20 60 100 0 20 40 60 80 100 120 100 500 1000 Timing (ms) Image Size (KB) DES Encryption Timing DES Algorithm 50 60 80 0 20 40 60 80 100 120 100 500 1000 Timing (ms) Image Size (KB) AES Encryption Timing AES Algorithm 30 40 70 0 20 40 60 80 100 120 100 500 1000 Timing (ms) Image Size (KB)

The simulation results for this comparison shown in figure .The results shows the superiority of AES algorithm over the other algorithms in terms of the throughput of encryption and decryption process. Because more throughput and more speed. Shows that for the size of 1, 5, 10 MB, the encryption timing is 50, 60, 80 milliseconds respectively. As the size of image increased the encryption time is also increased in AES algorithm.

Table 4.1 Shows that for the size of 1, 5, 10 MB, the AES encryption and Decryption timing

FILE Name	File Size (MB)	AES Enc. Time	AES Dec. Time
file1.dat	1	765	200
file5.dat	5	1326	606
file10.dat	10	2589	1251

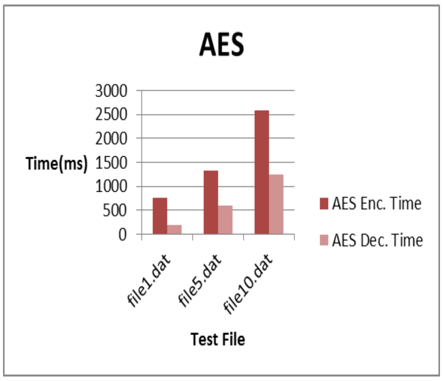

Fig. 1: AES encryption and Decryption timing

showed that AES has a very good performance compared to other algorithms. Also it showed that AES has a better performance than 3DES and DES.

Table 4.2 Shows that for the size of 1, 5, 10 MB, the AES ECC encryption and Decryption timing

FILE Name	File Size (MB)	ECC Enc. Time	ECC Dec. Time
file1.dat	1	391	229
file5.dat	5	638	1091
file10.dat	10	1199	2782

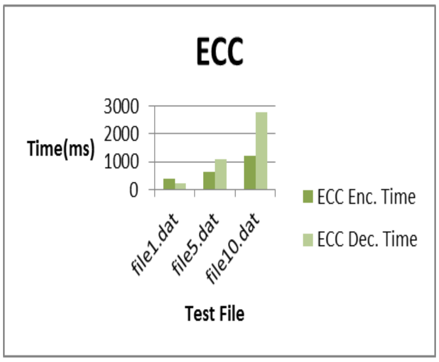

Fig. 2: AES based ECC encryption and Decryption timing

Table 4.3 Shows that for the size of 1, 5, 10 MB, the AES Hashing encryption and Decryption timing

FILE Name	File Size (MB)	Hashing Eec ECC Time	Hashing Dec ECC Time
file1.dat	1	20	13
file5.dat	5	55	61
file10.dat	10	112	127

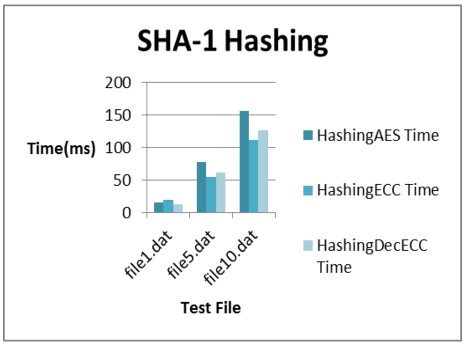

Fig. 3: AES based SHA encryption and Decryption timing

4.2 DES Based approach using Cloud Computing

One of the major issue in today's era so to enhance security we have cryptographic algorithms. In this thesis implementation o DES cryptographic algorithms on two different platform using JAVA has taken into consideration. By this implementation, performance analysis of these two algorithms has completed. Performance of these two algorithms depends upon various factors like no. of rounds, key size and etc., but in this experimental analysis performance is evaluated considering two parameters:-

1. Encryption Time
2. Decryption Time

Now click on select file, by this upload the file which we have to encrypt. After this two keys are generated simultaneously (DES secret key and SHA-1 Hash key) . Dailogue box appears "File successfully uploaded" after uploading of file.

Experimental Design of Time Consumption

Figure show the four encryption algorithms namely the DES algorithms. They are showing the time consumption of each compared algorithm in seconds when varying the size of data samples

Several performance metrics are collected:

1- DES encryption time and DES decryption time
2- ECC encryption time and ECC decryption time
3- Hashing ECC encryption time and Hashing ECC decryption time

Table 4.4.Shows that for the size of 1, 5, 10 MB, the DES encryption and Decryption timing

File Name	File Size (MB)	DES Enc. Time	DES Dec. Time
File1.dat	1	1950	580
File5.dat	5	3541	1927
File10.dat	10	5242	3386

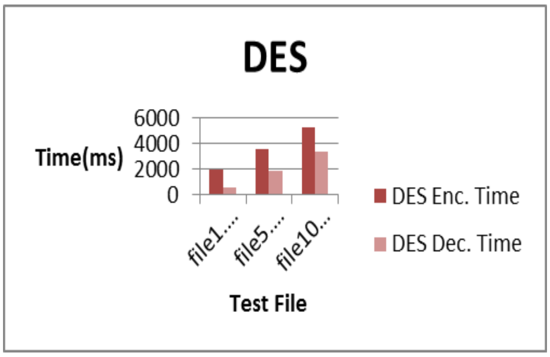

Fig. 4: DES based encryption and Decryption timing

Table 4.5 Shows that for the size of 1, 5, 10 MB, the DES ECC encryption and Decryption timing

FILE Name	File Size (MB)	ECC Enc. Time	ECC Dec. Time
File1.dat	1	2050	622
File5.dat	5	2573	4179
File10.dat	10	4403	4886

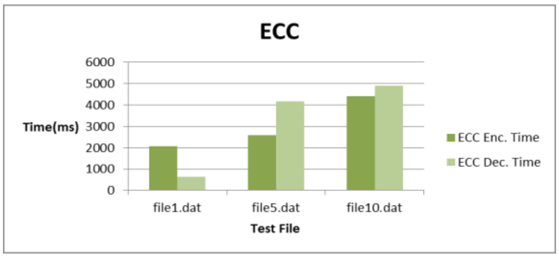

Fig. 5: DES based ECC encryption and Decryption timing

The encryption time is considered the time that an encryption algorithm takes to produces encrypted image (cipher) from original image. Comparisons analyses of the results of the selected different encryption scheme are performed.

Shows that for the size of 1, 5, 10 MB, the encryption timing is 20, 60, 100 milliseconds respectively. As the size of image increased the encryption time is also increased in DES algorithm.

Table 4.7 Shows that for the size of 1, 5, 10 MB, the DES Hashing encryption and Decryption timing

File name	File Size (MB)	Hashing Eec ECC Time	Hashing Dec ECC Time
File1.dat	1	33	30
File5.dat	5	149	237
File10.dat	10	238	248

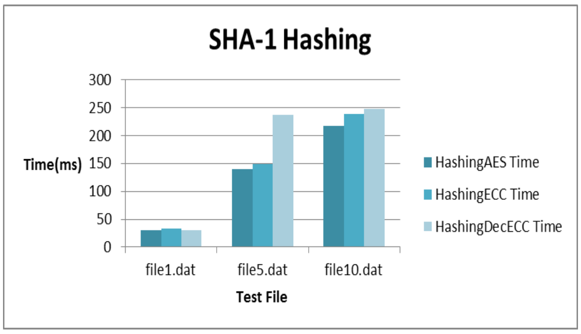

Fig. 6: DES based SHA encryption and Decryption timing

Shows that for the size of 1, 5, 10MB, the decryption timing is 10,40,80 milliseconds respectively. As the size of image increased the decryption time is also increased in DES algorithm.

V. CONCLUSION AND FUTURE SCOPE

In this paper ,Safety of information and confidence delinquent has continuously stayed a main and perplexing subject in cloud computing. This paper efforts to fact available benefits and safety anxieties of cloud computing and concentrating on evading third party examiners for information reliability checkered. Execution of projected convenience, which calculates hash values of document at the client's adjacent, can remove the requirement of third party examiners. The subsequent hash values after this convenience is kept at safe local hash source. The information document can be recovered back when desirable and squared aimed at some influences among parties complicated by re-computing and correspond the hash consequence through the pre-computed hash value

In the future, we will lengthen our model by given mistake localization and diminish. Protectedcustomerverification with fusion of AES and Blowfish for encoding/Decoding has probableinfluence not only on verification but also on recordsabove the cloud by means ofentrance control tools. By joining ECC and DH provideshealthiersafety and proceedsless time for encoding

VI. REFERENCES

[1]. KaziZunnurhain and Susan V. Vrbsky"Security Attacks and Solutions in Clouds"IEEE 2015

[2]. JiaXu, Jia Yan, Liang He, Purui Su, DengguoFeng, "CloudSEC: A Cloud Construction for Composing Collaborative security Services". In 2nd IEEE International Conference on Cloud Computing Technology and Science.pp. 703-711, IEEE, 2010.

[3]. SamanTaghaviZargar, James B. D. Joshi, "A Collaborative Approach to Facilitate Intrusion Detection and Response against DDoS Attacks". In the Proceedings of the 6th international Conference on Collaborative Computing: Networking, Applications &worksharing ,collaboratecom, Chicago, USA. October 2010.

[4]. Pritesh Jain, DheerajRane, ShyamPatidar, "A survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Combination in Renal Environment", In World Congress on Information and Communication Technologies. pp. 456-461, IEEE, 2011.

[5]. Aderemi A. Atayero, OluwaseyiFeyisetan,"Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", In Journal of Emerging Trends in Computing and Information Sciences, Vol-2, No.10, pp.546-552, October 2011

[6]. Pengfei You, YuxingPeng, Weidong Liu, ShoufuXue, "Security Issues and Solutions in Cloud Computing". In 32nd International Conference on Distributed Computing System Workshops, pp.573-577, 2012 (2012)

[7]. W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, M.t. Abdullaha, "Cloud-Based Intrusion Detection Service Framework". In the Proceedings of the International Conference on Cyber Security, pp. 213-218, IEEE, June 2012.

[8]. Abhishek Jain, Ashwani Kumar Singh, "Distributed Denial of Service (DDOS) Attacks – Classification And Implications". In Journal of Information and Operations Management, ISSN: 0976-7754 & E-ISSN: 0976-7762, Vol. 3, Issue 1, pp 136-140, 2012

[9]. http://www.symantec.com/connect/articles/justifying-expense-ids-part-one-overview-rois-ids

[10]. //netsecurity.about.com/cs/hackertools/a/aa030504.htm

[11]. Sanjay B Ankali, Dr. D V Ashoka, "Detection Architecture of Request Layer DDoS Attack for Internet". In International Journal of Advanced Networking and Applications, Vol-o3, Issue: 01, pp. 984-990, 2011.

[12]. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalasi, "Cloud Compuating- The business perspective", Decision Support Systems, Vol. 51(1), pp. 176-189, 2011.

[13]. The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[14]. I. Brandic, "Towards self-manageable cloud services", IEEE International Conference on Computer Software and Applications, pp. 128-133, 2009.

[15]. M. Alhamad, T. Dillon and E. Chang, "A survey on SLA and performance measurement in cloud computing", On the Move to Meaningful Internet Systems: OTM 2011, Springer Berlin Heidelberg, pp. 469-477, 2011.

[16]. C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The characteristics of cloud computing", IEEE International Conference on Parallel Processing Workshops, pp. 275-279, 2010.

[17]. A. Younge, R. Henschel, T. Brown, G. Laszewski, J. Qiu and G. Fox, "Analysis of virtualization technologies for high performance computing environments", IEEE International Conference on Cloud Computing, pp. 9-16, 2011.

[18]. R. Mietzner, T. Unger, R. Titze and F. Leymann, "Combining different multi-tenancy patterns in service-oriented applications", IEEE International Conference on Enterprise Distributed Object Computing , pp. 131-140, 2009.

[19]. IBM, "Fundamentals of Cloud Computing", Instructor Guide ERC 1.0, pp.17-230, Nov. 2010.

[20]. M. Rosenblum, "VMware's Virtual Platform", Proceedings of Hot Chips , pp. 185-196. 1999.

[21]. Q. Zhang, L. Cheng and R. Boutaba,, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Services and Applications, Vol. 1(1), 7-18, 2010.

[22]. F. Chen, J. Schneider, Y. Yang, J. Grundy and Q. He, "An energy consumption model and analysis tool for cloud computing environments ", International workshop on Green and Sustainable Software, pp. 45- 50, 2012.

[23]. Monjur Ahmed and Mohammad Ashraf Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[24]. Randy Marchany , VA Tech IT Security, "Cloud Computing Security Issues", Virginia tech Invent the future Copyright marchany 2010.

[25]. Kuyoro S. O., Ibikunle F. and Awodele O., "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[26]. DimitrisZissis and DimitriosLekkas, "Addressing cloud computing security issues" , Future Generations Computer Systems , Volume 28, issue 3, March 2012, Pages 583-592.

[27]. mer Khalid, Abdul Ghafoor, MisbahIrum and Muhammad AwaisShibli, "Cloud based Secure and Privacy Enhanced Authentication & Authorization Protocol", 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013, Procedia Computer Science 22 (2013) 680 – 688.