iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.52532

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Enhancing the Security of Cloud using Fault Resolving Script (FRS)

Prof. A. Kannaki[1], Vasantha Azhagu[2], K. Prakash[3], I. Somasundaran[4], J.Tamilarasan[5], S. Yogeshwaran[6]
[1]*Associate Professor & Head/CSE,* [2,3,4,5,6]*Final Year, Computer Science Engineering, Achariya College of Engineering Technology*

Abstract: ***Cloud computing has made individual users lives and the work of businesses much easier by providing data storage services at very low costs. Individual users can store and access their data via a shared cloud storage service from any location at any time. A cloud attack is a cyber attack that targets cloud-based service platforms such as computing, storage, or hosted application ina Platform as a Service (PaaS) or Softwareas a Service (SaaS) model. A majority of breaches and cyber attacks in cloudinfrastructure are the result of human error and misconfiguration vulnerabilities customer-centric tools are crucial to mitigating these threats. Yet existing cloud security models are largely unable to address these issues. We propose Fault ResolvingScript (FRS) techniques to address the challenges. FRS applies the principle of chaos engineering to cloud security.***
Keywords: Platform as a Service, Software as a Service, Fault Resolving Script.

I. INTRODUCTION

Cloud computing is the term for data storageusing Internet-based technology. This strategy is becoming more popular due to factors including time, money, distributed complex sourcing, quicker innovation delivery, and rising complexity. A computer user can access information technology (IT) services, such as servers, applications, and data storage, via cloud computing without needing to understand the underlyingtechnology or even to own the infrastructure.Similar to the power grid, pooled resources, software, and information are made available to computers and other devices on demand through cloud computing, which is Internet-based computing. Grid computing, distributed computing, parallel computing,and other established computing and network technologies are all combined in cloud computing to create something new. Cloud computing is the term for data storageusing Internet-based technology.

This strategy is becoming more popular due to factors including time, money, distributed complex sourcing, quicker innovation delivery, and rising complexity. A computer user can access Information Technology (IT)services, such as servers, applications, and data storage, via cloud computing without needing to understand the underlyingtechnology or even to own the infrastructure.Similar to the power grid, pooled resources, software, and information are made available to computers and other devices on demand through cloud computing, which is Internet-based computing. Grid computing, distributed computing, parallel computing,and other established computing and network technologies are all combined in cloud computing to create something new. It seeks to paradigmatize a precise system withsubstantial computational power for theduration of a considerable

The first advantage of cloud computing is that it lowers the cost of the gear that users have purchased via the cloud. Since the data is already stored elsewhere, there is no need to store it on the end user's computer. Therefore, you are just renting the assets in accordance with your needs rather than purchasing the entire infrastructure needed to run the process and save a large amount of data.

II. LITERATURE SURVEY

In 2018 Joseph Selvanayagam wrote a paper named Secure train storehouse on pall using Cryptography.(1) The end of this paper is to understand about the security trouble of stored train on pall using different ways of cryptography. In this paperauthor has described about the Asymmetric and symmetric ways which is one of thenotorious encryption and decryption ways. In this AES and DES ways has been described in detail, All the way of both the ways is been bandied in this paper. One further fashion which is bandied then RC- 2 Encryption Algorithm.

In 2018 caddy- hawing Lee wrote a paper named Data security in cloud computing using AES(2). In this paper they've bandied about the security pitfalls and identify the applicable security ways used to alleviatethem in cloud computing. In this paper they had bandied about data security in pall computing using AES under HEROKU cloud, After that the enforced a website as an operation for data security and in AES they enforced AES as data security algorithm.

In 2017 sarojinietal proposed a fashion known as Enhanced collective Trusted Access Control Algorithm (EMTACA). Thisfashion provides a collective trust for both cloud druggies and cloud service provider toavoid security affiliated issues cloud computing. The end of this paper is to propose a system which include EMTACA algorithm which can enhance guaranteed and trusted and character- grounded cloud services among the druggies in a cloud terrain the result of this paper showed data confidentiality, integrity, vacuity which is three most important aspect of data security was achieved.

III. PROPOSED SYSTEM

To ensure the safety of user data, we propose a hybrid algorithm that combines the strengths of Camellia and RSA cryptography. This system is designed to protect sensitiveinformation such as user passwords, credit card details and other personal information. Here are the steps I would take to implement the proposed system:

User Registration: When a user registers for an account, first the password is encrypted using her Camellia encryption algorithm. Camellia is a symmetric key block cipher thatoffers high security and performance. Encrypted passwords are stored in the database.

User Authentication: When a user logs in,the encrypted password is retrieved from thedatabase and decrypted using the Camellia algorithm. The decrypted password is compared with the password entered by the user. If they match, the user will be able to access their account.

Data Encryption: When users enter personal information such as credit card details, that information is encrypted using the RSA encryption algorithm. RSA is an asymmetric key encryption algorithm that uses public and private keys to encrypt and decrypt data. Theuser's public key is used to encrypt the data. Data can only be decrypted with the private key.

Data Storage: Encrypted personalinformation is stored in a database. This makesit impossible for a hacker to access yourdatabase, as the data is encrypted with his RSA. Five. Data Retrieval: When a user wants to view their personal information, encrypted data is retrieved from the database and sent tothe user's device. The user's private key is then used to decrypt the data presented to the user. Combining the strength of Camellia and RSA encryption methods, users can ensure the safety of her data from external and internal threats. The system also ensures that userpasswords and personal information areprotected from unauthorized access

IV. RSA ALGORITHM

The most generally used asymmetric algorithm is Rivets-Shamir-Adelman (RSA). It was introduced by its three formulators, RonaldRivest, AdiShamir and LeonardAdelman in 1977. It's substantially used in crucial distribution and digital hand processes. It's grounded on the presumed complexness of factoring large integers. An asymmetric algorithm has set of crucial one is public and another one private key. The RSA algorithm involves three way Generation of key, Encryption of data, Decryption of data RSA involve a crucial combination similar as public key and a private key. The public key can be known to everyone and is used for cracking dispatches. Dispatches translated with the public key can only be deciphered using the private key. RSA algorithm involves three ways

1) Key Generation
2) Encryption
3) Decryption

a) *Key Generation:* Before the data is translated, crucial generation should be done. This process is done between the cloud service provider andthe stoner.

V. CAMELLIA ALGORITHM

In cryptography, Camellia is a symmetrickey block cipher with a block size of 128 bits and crucial sizes of 128, 192 and 256 bits. It was concertedly developed by Mitsubishi Electric and NTT of Japan. The cipher has been approved for use by the ISO EC, the European Union's NESSIE design and the Japanese CRYPTREC design. The cipher has security situations and processing capacities similar to the Advanced Encryption Standard. The cipher was designed to be suitable for both software and tackle executions, from low- cost smart cards to high- speed network systems. It's part of the Transport Layer Security (TLS) cryptographic protocol designed to give dispatches security over a computer network similar as the Internet. The cipher was named for the flower Camellia japonica, which is known for being long- lived as well as because the cipher was developed in Japan. Camellia is considered a ultramodern, safe cipher. Indeed using the lower crucial size option(128bits), it's considered infeasible to break it by brute- force attack on the keys with current technology. There are no known successful attacks that weakenthe cipher vastly.

The cipher has been approved for use by the ISO/ IEC, the European Union's NESSIE design and the Japanese CRYPTREC design. The Japanese cipher has security situations and processing capacities similar to the AES Rijndael cipher Camellia is a block cipher which can be fully defined by minimum systems of multivariate polynomial (plague) The Camellia(as well as AES) S- boxes can be described by a system of 23 quadratic equations in 80 terms. The crucial schedule can be described by 1,120 equations in 768 variables using 3,328 direct and quadraticterms. The entire block cipher can bedescribed by 5,104 equations in 2,816 variables using 14,592 direct and quadratic terms in total, 6,224 equations in 3,584 variables using 17,920 direct and quadratic terms are needed. The number of free terms is 11,696, which is roughly the same number as for AES. Theoretically, similar parcels might make it possible to break Camellia(and AES) using an algebraic attack, similar as extended meager linearization, in the future, handed that the attack becomes do able

Table 1:Comparison table for RSA and AES

	Parameters	AES	RSA
i.	Computation Time	Faster	Slower
ii.	Memory Utilization	Requires moderate memory space	Requires more memory space
iii.	SecurityLevel	Excellent Security	Least Secure

VI. HASHING

Hashing is also one of the fashions to secure your data on cloud. It's a function whichinduces a fixed length result, which is also called hash- value or hash. It's a fine algorithm that maps data of arbitrary size to a hash of fixed size. Hash functions are used for Digital autographs, Communication Authentication law and other form of authentication. There are two main types of Hashing ways which are MD5, SHA Hash functions are also used to make caches for large data sets stored in slow media. A cache is generally simpler than a hashed hunt table, since any collision can be resolved by discarding or writing back the aged of the two colliding particulars. The effectiveness of mapping depends of the effectiveness of the hash function used. MD5 The Message-Digest hashing algorithm is hash functionproducing a 128- bit hash value. The input communication in this is divided into knob of 512 bits blocks. The processing of communication takes place in four different stateside nominated as "Round" and eachround have 16 analogous operations. SHA the Secure Hash Algorithm are the part of cryptographic hash functions. There are different performances of SHA algorithm some of the exemplifications are SHA-0, SHA- 1,SHA- 2, SHA- 3.

1) SHA It's the original interpretation of 160- bit hash function but it was withdrawn veritably soon because of some significant excrescence and replaced by SHA-1.

2) SHA-1 It's also a 160- bit hash function which resembles the MD5.This was designed by National Security Agency(NSA) so that it can come a part of Digital hand Algorithm. Some cryptographic issues were reported in this algorithm so it wasn't approved substantially after 2010.

3) SHA- 2 It's the different interpretation of SHA family as it consists of two analogous hash functions but with different block size known as SHA- 256 and SHA- 512, they differ in word- size SHA- 256 uses 32- byte words and SHA- 512 uses 64- byte words.

4) SHA-3 It's also called a "keccak", It supports the same length as SHA- 2 just the difference is that its internal structure varies from all other SHA- family.

VIII. OUTPUT

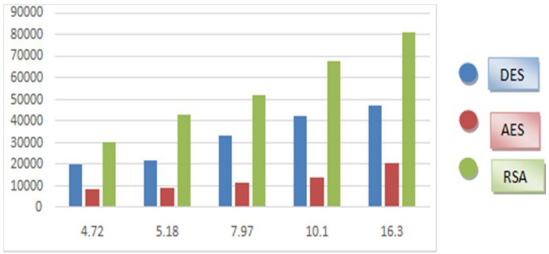


Fig 1: Comparative status of EncryptionTime among AES, DES and RSA

By analyzing Fig 1: which shows time taken for encryption on various sizes of file by three algorithms. AES and RSAalgorithm show very minor difference in time taken for encryption process.

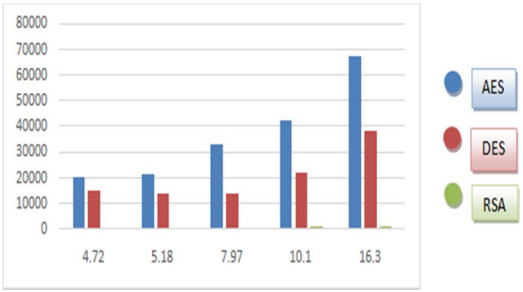


Fig2: Comparative status of Decryption time among AES, DES and RSA

By analyzing Fig 2: which shows time taken for decryption on various sizes of file by three algorithms. RSA algorithm takes longer time compare to time taken by AES and DES algorithm. AES takes the least time to decrypt.

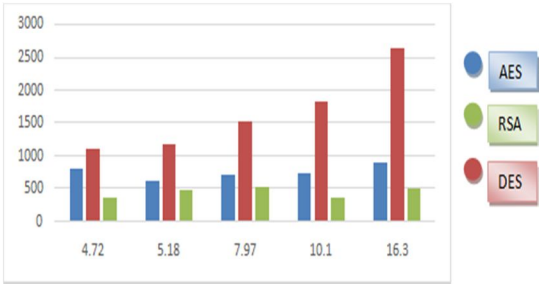


Fig 3: Comparative status of Memory utilization (Encryption) among AES, DESand RSA

BigOanalysis is used to verify the complexity based on the efficiency of the algorithm, i.e., it tests for space and time, in order to assess the efficiency of acryptographic method based on memory utilization. Regardless of the input, AES andDES typically only operate on set block sizes and take around the same amount of time. As a result, they run on O(1) since the key size determines how quickly they execute rather than the file size. On the otherhand, RSA, Because it Encrypts and Decrypts based on the size of file. Encryption and Decryption take O(n) time.

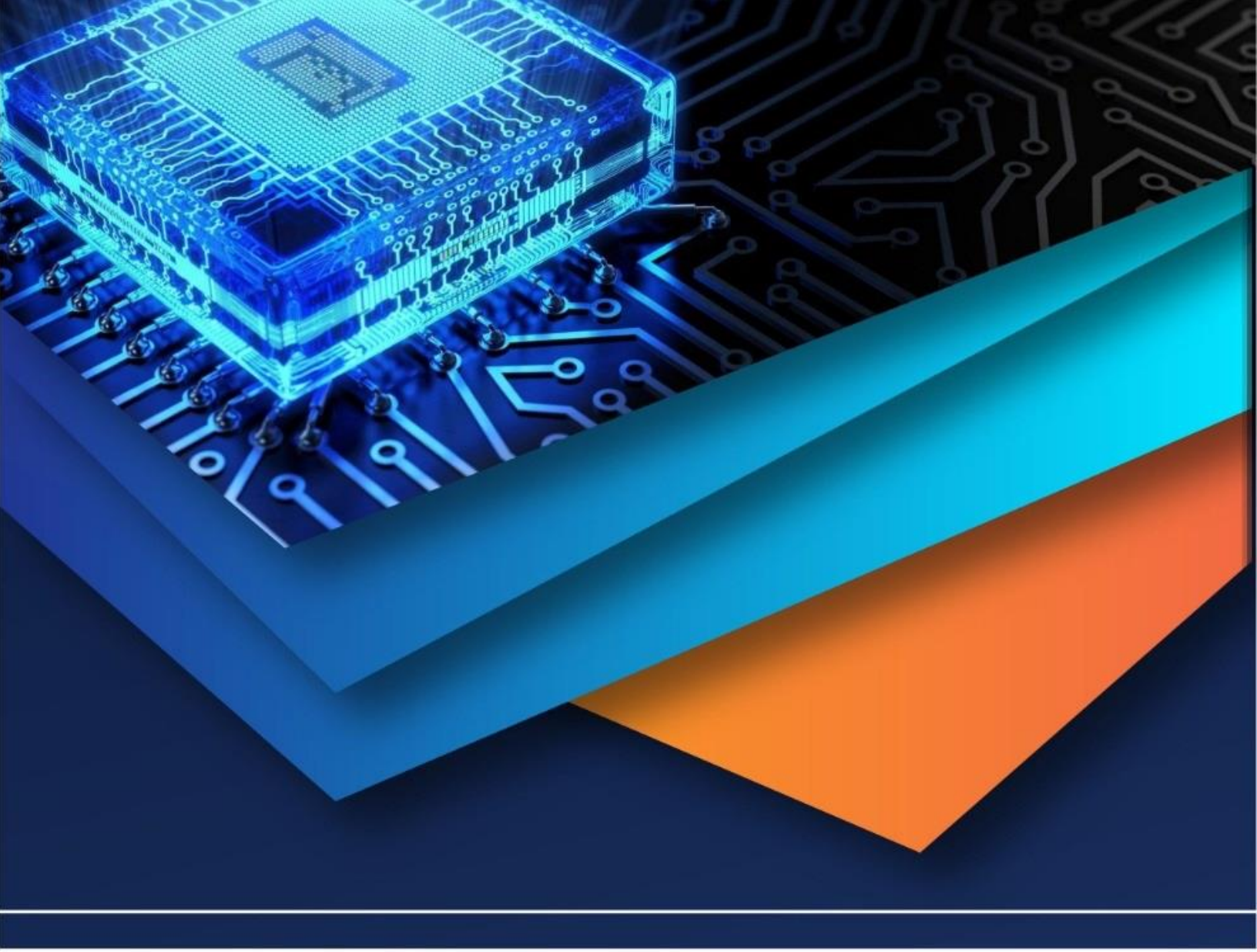
IX. CONCLUSION

Cloud computing is a new evolving way where on demand computing is available. Then cloud services are fluently available on pay- per- use base. By putting the data on cloud it decreases the control on data by the organization, therefore we've to give the new security ways to cover that data that relies on some of the cryptography algorithms, So that only authenticated stonercan pierce the data irrespective of thenumber of druggies who can capture it. Data security is handed by enforcing RSA algorithm. This paper represents perpetrationof RSA and CAMELLIA through encryption and decryption procedure

.unborn compass should be in RSA cryptography in comparison of another cryptography algorithm, and developing another algorithm, incorporating two algorithms which give further security.

REFERENCES

[1] S. Kumari and J. Chawla, Comparative Analysis on Different Parameters ofEncryption Algorithms for Information Security, International Journal of Innovations& Advancement in Computer Science(IJIACS), Volume 4, Special Issue, pp. 123-129, 2015..
[2] S. Gurpreet and Supriya,A Study of Encryption Algorithms (RSA, DES, 3DESand AES) for Information SecurityInternational Journal of ComputerApplications, Volume6, Issue 19, pp. 33-38,2013.
[3] H.O.Alanazi,B.B.Zaidan,A.A.Zaidn, H.A.Jalab,M.Shabbir and Y.Al-Nabhani,NewComparative Study Between DES, 3DES andAES within Nine Factors", Journal ofComputing, Volume 2, Issue 3, pp.152-157,2010.
[4] N.Singhaland J.P.S.Raina,Comparative Analysis of AESand RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology, 177-181,2011.
[5] K.Ajah, M.Singh and P. Bansel, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multimode Network. International Journal of Engineering andTechnology, Volume 2, Issue 1, pp.87-92,2012.
[6] DiaaSalama A. Elminaam, M. Hatem and Mohi M.Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms: IJCSNS International Journal of Computer Science and Network Security, Volume 8, Issue 12, pp.280- 286, 2008.
[7] S.Lalit and R.Bharti, Comparison among different Cryptographic Algorithms: Neighborhood-Generated Keys International Journal of Computer Applications (0975 – 8887), Volume 73, Issue 5, pp. 144-153, 2013.
[8] Pasmavathi B. and Ranjitha S.A Survey Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique: International Journal of Science and Research (IJSR) Volume 2, Issue 4, pp. 170-174,2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY