International Journal of Engineering & Technology, 7 (4.36) (2018) 773-776

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Performance Analysis of Aes and 3des for Implementing Multi Level Authentication in Cloud Through Rest Api

M.J. Balachandran[1*], P.Sujatha[2]

[1]Research Scholar, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies, Chennai, India.
[2]Professor, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies, Chennai, India.
E-mail:suja.research@gmail.com
**Corresponding author E-mail:mjbalachandran@yahoo.co.in*

Abstract

Last couple of decades, internet usage has been changed each and every technology domain. This has lead to implementation and accommodation of cloud computing. As the Cloud has the nature of sharing the data, it led to various types of security attacks. Hence security mechanisms which has various features/types are needed and hence security breaches can be prevented. Authentication is one of the vital techniques playing a major role in security part. Cloud Computing verifies the identification of a user during the process of accessing the services from cloud servers. Different authentication techniques are used to verify the user's identity before granting the access to them. This paper analyze the performance of AES and 3DES algorithms and find out the best suit for implementing multi level authentication in cloud. Based on execution time, request and response time against the concurrent user load and file size, AES is faster, more secure and safer than 3DES.

Keywords: *Multi factor authentication, application programming interface, insecure API, & Cloud computing security challenges.*

1. Introduction

APIs are strategic important for our business. It facilitates innovation and agility. A secure API guarantees the process of protecting the information by allowing only to its authenticated Users, Servers and Apps, that are authorized to access it. Similarly, it also secures the upstandingness of the information shared by the clients and also the servers. Because of this, it will process only the respective information post verification and ensures that this is not edited by a third party. To assure these two features of securities, calling systems and its respective end-users to be identified as a pre-requisite. This also applicable to those calls whenever API is making to third party Servers. An API without losing information it is to be made available as this is to process the requests in a reliable fashion.

Any authenticated user is needed to login before exploitating the services of Cloud or availing the sensitive information in the cloud. There are couple of issues for the account as well as password based, this authentication isn't privacy-preserving but it is to be very much considered in cloud systems. Secondly, with the spyware Sign-in credentials from the web-browser would be known to the hacker. Using access control model which is known as attribute-based access management which will help to tackle the issue. It provides authentication without any strong validation mechanism.

The intention of this research is to implement multilevel authentication in cloud through REST API. As stronger encryption leads to more security, encryption is one of the main phases in this research.

Hence, this paper analyses the performance of AES and 3DES and concludes that AES provides stronger encryption than 3DES in terms of execution time, request and response time against the concurrent user load and file size.

2. Literature survey

In this paper, Author Huma [1] explains about various techniques involving Multi-level authentication to ensure more secured information in cloud computing environment, here authentication techniques with various combinations have been used. This system is highly secure because it is not only validating the login credential combination but also needs another authentication factor which is bio-metric, this includes finger print and vein of a palm. The research aimed to analyse and handle the data of biometric in a secured manner. In this, fingerprint data is stored centrally on the cloud server and the palm vein data in smart cards with multi-component. Beyond the authentication of user name and password, mobile trusted module technique is used, this ensures the reliability and integrity of a mobile platform. Second technique is Single Sign On (SSO). An identity of a user is proved by using the Private key. Fourth one is Biometric authentication, it is of two types: behavioural and physiological. 1. Behavioural biometric involves signatures, voice prints and keystrokes are used. 2. Physiological biometric involves authentication, hands, palm/finger-print, retina, faces, iris and retina are used.

Manjushree.C.V et.al [2] briefed about current security mechanisms and its respective challenges. Primarily S2N is a tool which is more secure and it is used in Amazon web services (AWS) and a new implementation of TLS encryption protocol former openSSL. TLS protocol provides integrity and privacy between two communicating protocol applications. Secondly, data of Threshold cryptography encrypted using public key and private key which is shared among the appropriate authenticated users but they are lacked in some ways, violation of data privacy because of collision attack and heavy computation. To overcome

such attack single key is shared to the group of users to perform encryption and decryption. Third is Log files analysis method, Log file contains a data generated from different transactions during navigating from one web site or application to another. Fourth is SSH (secure socket shell) It is a network protocol of cryptographic which gives authentication and encryption between two systems when it is connected through web.
The challenges here are poor key management, API attacks, public and user credentials. Fifth is REST (Representational state transfer) It is a communication of data between client and cloud providers using HTTP protocol. In REST each and every component is a resource and these are accessed by using standard HTTP methods. Limitations are, there are no uniform standards regarding policy language and for the policy implementation users are to deal with specific policy types for system accommodation. Sixth is Access control mechanisms, used for controlling accessing of data in cloud computing is attribute based encryption. Lastly Bio inspired model which has the capability of processing complex information and providing solutions to many problems. The limitations in this model are, latency is decreased and performance is increased, data sharing between multiple users cannot be used.
Shreya Gawade et.al [3] here explained about how BioAaaS based authentication scheme is efficient in biometric authentication. This involves, Enrolment and Verification. Whenever biometric information is provided by the user i.e. fingerprint to the biometric sensor, which leads in converting the data of biometric into a binary string. Elimination of redundancy is executed by the feature extractor. Service provider's database stores the feature of vector. During the process of verification, execution of same mentioned steps will be executed whenever a user tries to log in into the remote cloud server. When a new user required to access the Cloud, he/she must register by using their fingerprints. Once it is registered they become a valid user and can login to the cloud. Reverse Circle Cipher algorithm is used to store and encrypt the fingerprint image. Based on the above system architecture, authors are proposing a biometric authentication mechanism which gives a secure login to the cloud server and verifying the user even when there is a change of fingerprint. This is executed by an Outsourceable two party Privacy preserving Biometric Authentication method.
A. Anuradha et.al [4] Author has explained on the Image steganography which is most robust process of passing the message secretly. It is relatively good techniques than watermarking and cryptography, text/ audio based steganography. The proposed model has the implementation of steganography based on the Secret key where the communication methodology is known, but during the same time secret key is unknown, thesis different from Pure steganography hence implementation of Kerckhoff's principle. The value addition is, an generation of an unique ID based on the image of finger print which is used as steganography key in creating the image of stego as this protects the uniqueness during embedding process.
Syed Luqman Quadri et.al [5], has done research on cloud and bio metrics while implementing bio metric authentication as a service. He also explained the usage of cloud and biometrics in different industries and how its usage has exponentially increased in the last 10 years. They have done a case study of finger print registration and verification, it requires a large storage volume and high computational power to make the authentication service robust and reliable. Author has explained on various advantages of using Biometrics as a service: Availability, which guarantees 99% availability of a system.

3. Methodology

3.1.Advanced Encryption Standard [AES]

AES encryption is carried out on the basis of per-block which determines the plaintext as input and cipher text as output. As AES is a symmetric algorithm, encryption and decryption uses the same key. The AES operation is a 4 X 4 column major order matrix of bytes. The key size of the cipher indicates the repetitions to place the plaintext through cipher for the conversion of cipher text.

3.2.How AES algorithm works into our implementation

- Derive the set of round keys from the cipher key.
- Initialization of plaintext or an array of block data.
- Addition of initial round key to the initiating state array.
- Execution of nine rounds of state manipulation.
- Execution of tenth and final lap of state manipulation

AES cycles break down process are given below.
128-bit key requires 10 rounds of execution
192-bit key requires 12 rounds of execution
256-bit key requires 14 rounds of execution
In this research, key size of 128 bits is chosen because in AES the size of each block is usually measured in bits. The operation of 128 bits of plaintext to produce 128 bits of cipher text and for research purpose it is easy to conclude on the minimum scale.

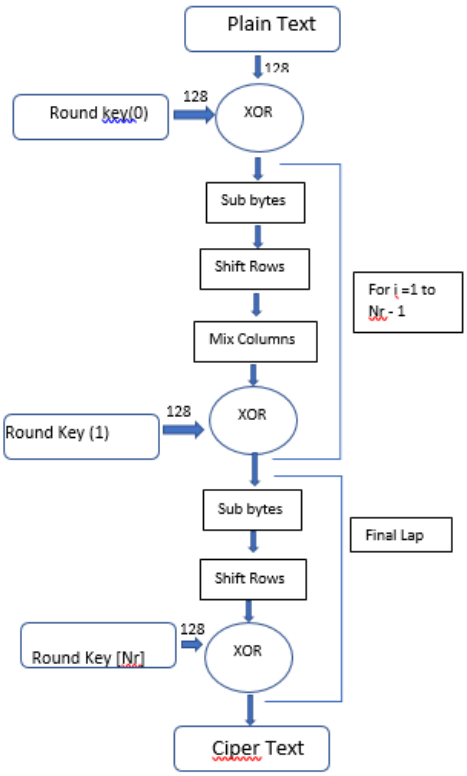

Fig. 1: AES Encryption process

Stronger encryptions are performed on the provision of longer keys, the strength is based on the cost of performance, i.e., it takes longer to encrypt.

4. Comparative analysis of AES and 3DES

AES data encryption is a cryptographic algorithm, and its main strength is based on various key lengths. AES permits to choose 128, 192 or 256 bit, making it exponentially stronger than the 64-bit key of 3DES.

3DES internally use the 112 bits out of those 128 bits; must have length 16 or 24 bytes. Here, the key itself encoded into bytes, stored and exchanged.

Some security issues with 3DES is, when the encryption is more than 32 GB with a single key, the limit is much higher with AES and this is due to the block size; 64-bit blocks are used by 3DES which leads to trouble post processing 264/2 blocks, i.e. 32 gigabytes; 128-bit blocks used by AES, for a limit of 2128/2 blocks, i.e. 268 bytes Hence, AES is also noticeably faster than 3DES. The following table shows the comparison of AES and 3DES algorithms.

Table 1: Comparative Analysis of AES and 3DES

AES	3DES
AES is a symmetric block cipher algorithm which is used for encryption. It encrypts data on a per-block basis. The "blocks" are measured in bits determine the input of plaintext and output of ciphertext.	3DES is a way to reuse DES implementations, by chaining three instances of DES with different keys. 3DES is also secure because it requires 2112 operations which is widely accepted technology
AES uses keys of 128, 192 or 256 bits, although, 128 bit keys provide sufficient strength today. It uses 128 bit blocks,	3DES also uses the same block length of 64 bits, half the size that of AES at 128 bits. It it requires 2112 operations which is widely accepted technology
AES cycles break down process are, 10 rounds are required for a 128-bit key 12 Rounds are required for a 192-bit key 14 Rounds are required for a 256-bit key	Encrypt the plaintext blocks using single DES with key K1. Decrypt the output of step 1 using single DES with key K2. Encrypt the output of step 2 using single DES with key K3. Final output is the ciphertext. Decryption of a ciphertext is a reverse process
AES is efficient in both software and hardware implementations.	3DES is very slow especially in software implementations because DES was designed for performance in hardware.
AES uses a totally different encryption	3DES uses identical encryption to DES
AES has stronger encryption keys	3DES has shorter and weaker encryption keys
AES uses non-repeating encryption keys	3DES uses repeating encryption keys

Below experimental research provides the tabular and pictorial representation based on Symmetric algorithm which is executed between proposed system with AES and against 3DES.

Table 2: Turnaround Time based on Input File Size between AES and 3DES

Input File Size (bytes)	3DES (Milli Sec)	AES (Milli Sec)
21,427	6	4
33,002	12	5
46,941	16	7
58,892	21	12
70,645	25	14
107,825	50	27
168,901	62	32
232,398	84	47
Avg Time	34.5	18.5
Avg Bytes/ Milli sec	2,421	5,430

Table 2 depicts the execution time of 3DES and AES for the given input file. The total request time has been calculated by providing different file sizes as input and recorded against the encryption and decryption processes of the above said algorithms. 'X'-Axis denotes increase in file size and "Y" axis denotes the time in milli-seconds. Average bytes per milli sec of AES is 5430 against 2431 of 3DES.

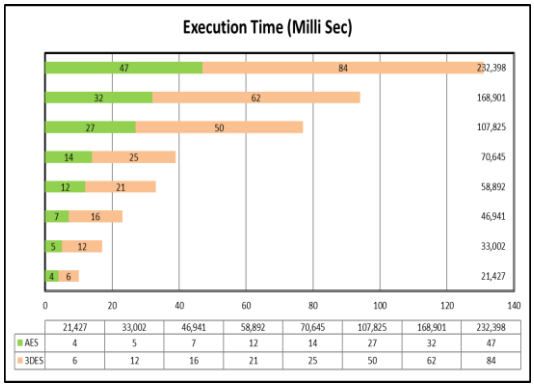

Fig. 2: Turnaround time comparison between AES and 3DES

The turnaround time has been analyzed based on two dimensions, one is based on the increase in number of users with the same file size while raising the request and the other analysis is based on response time. Comparison of Request and Response time of AES and 3DES are given as follows.

Table 3: Request Time based on Input File Size between AES and 3DES

No of Users/ File size	AES (Milli Sec)	3DES (Milli Sec)
2 / 500 MB	3	5
4 / 500 MB	4	6
6 / 500 MB	5	7
8 / 500 MB	8	10

The above table shows the total time taken between the submission of a program/process/thread/task and the return of the complete output to the customer/user. In the instance a single thread, a HTTP Request executes and set to wait for 1 second over and over. This means for each thread, we get 1 HIT (if everything goes off without a hitch).

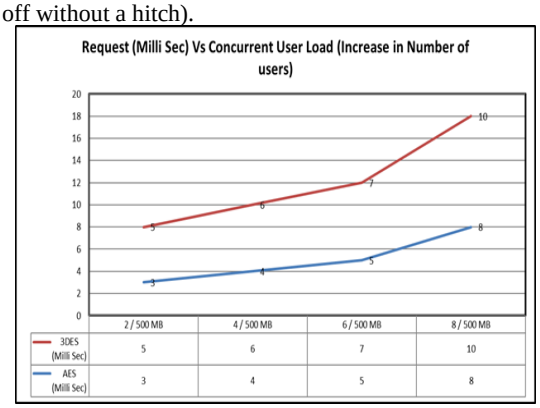

Fig. 3: Request per milli second Vs concurrent user load using 500 MB file size

Table 4: Response Time based on Input File Size between AES and 3DES

No of Users/ File size	AES (Milli Sec)	3DES (Milli Sec)
2 / 500 MB	3	4
4 / 500 MB	4	6
6 / 500 MB	5	7
8 / 500 MB	8	9

The above table shows the total time taken to process the 500MB file size with the increase in number of users on a gradual interval. The request and response time are same for AES whereas 3DES shows slight variation in millisec. The respective graph is shown in the below picture.

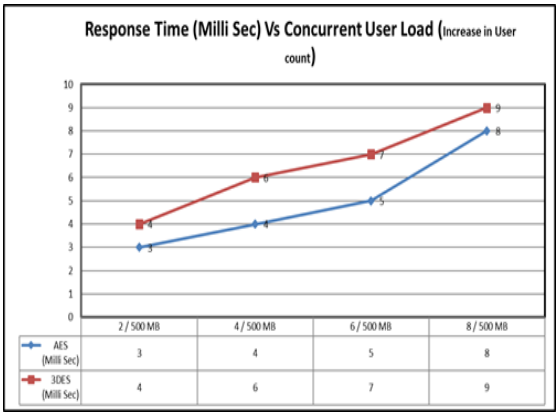

Fig. 4: Response per milli second Vs concurrent user load using 500 MB file size

Increase of request is based on the increase of load to the server which must be handled per second and subsequently raises the response times.

5. Conclusion

This paper analyses the performance of AES and 3DES algorithms and find out the best suit for implementing multi-level authentication in cloud. Based on execution time, request and response time against the concurrent user load, AES is faster, more secure and safer than 3DES. In Cloud based applications, Security of data has been increased by using AES Encryption algorithms

When using keys as 168-bit 3DES and 128-bit AES, it is not possible to find a private key. When a user forgets to log out and leaves the session active for some time and during this time when an attacker trying to access the system to open a file and steal the data, then the private key is required for the attacker.

In another situation, even though an un-auhorized entrant is successful in his/her attempt to break into the user system, and also able to somehow guess the private key leading to download the encrypted data but definitely it is not possible to access the original data.

The execution results showed that AES has a very good performance compared to 3DES algorithm to process the same amount of data. The response and request time were checked against the concurrent user load with increase in number of users count using 500 MB size, the marginal difference has been observed and specified above.

Most of the security mechanisms have some drawbacks or challenges here and there. Hence, it is concluded that it is essential to use AES with secured REST API for the multi-stage authentication using atleast one strong/secured biometric technique.

Future Work

The current research analysis is to identify the best and persistent mechanism for multi-stage authentication through cloud computing. In future, reliable various biometric mechanism is planned by the addition of explicit and secured type of biometric system and tries to make system more improving.

Acknowledgment

This paper is intended to analyze and implement the best security algorithm between AES and 3DES to overcome the challenges of current security and access related challenges through API. For this research I thank my guide Dr.P.Sujatha for her review and her motivational background helped to narrow down the analysis and research direction to the focused one

References

[1] Luo Y, Hongbo Z, Qingni S, Anbang R & Zhonghai W, "Restpl: Towards a request-oriented policy language for arbitrary restful apis", *IEEE International Conference on Web Services (ICWS)*, (2016), pp.666-671.

[2] Dindoliwala VJ & Rustom DM, "Survey on Security Mechanisms In NoSQL Databases", *International Journal of Advanced Research in Computer Science*, Vol.8, No.5, (2017).

[3] Gawade S, Anand B, Ashish R & Shweta M, "Biometric Authentication using Software as a Service in Cloud Computing", *International Journal Of Engineering And Computer Science*, Vol.6, No.3, (2017).

[4] Anuradha A &Hardik BP, "Biometric Based Security Model for Cloud Computing Using Image Steganography*", International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.7, No.1, (2017).

[5] Balachandran MJ, "Efficient Multi-Level Authentication for Cloud API based on RestPL", *International Journal of Computer Science and Information Security*", Vol.15, No.11, (2017).

[6] Syed LQA & Areeba K, "Cloud and Biometrics: The Future of Authentication", *International Journal of Advanced Research in Computer Science*, Vol.8, No.2, (2017).

[7] Ankita C & Neeraj S, "Multi-Level Authentication Technique for Accessing Cloud Services", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol.4, No.12, (2016).

[8] Soyjaudah KMS, Gianeswar R & Muhammad YK, "Cloud computing authentication using cancellable biometrics", *IEEE AFRICON*, (2013), pp.1-4.

[9] Eldefrawy MH, Khaled A & Muhammad KK, "OTP-based two-factor authentication using mobile phones", *IEEE Eighth International Conference on Information Technology: New Generations (ITNG)*, (2011), pp.327-331.

[10] Acharya S, Apoorva P & Pawar PY, "Two factor authentication using smartphone generated one time password", *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol.11, No.2, (2013), pp.85-90.

[11] Lee S, Ong I, Lim HT & Lee HJ, "Two factor authentication for cloud computing", *International Journal of KIMICS*, Vol.8, (2013), pp.427-433.

[12] Giradkar MS, Shraddha S & Choudhari NK, "A survey paper on Various biometric security system methods", *International Research Journal of Engineering and Technology*, (2016).

[13] Farooq H, "A Review on Cloud Computing Security Using Authentication Techniques", *International Journal of Advanced Research in Computer Science*, Vol.8, No.2, (2017).