International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

DATA SECURITY IN CLOUD COMPUTING THROUGH AES UNDER DRIVEHQ

Mr. K Sateesh[1*], R Aneesh[1], P L Chandana[2], V Deepika[3], T Sandeep Kumar[4]

[1]Associate Professor,Dept of Computer science & Engineering, Dhanekula Institute of Engineering & Technology, Ganguru, AP [1,2,3,4]B.Tech Student, Computer Science & Engineering, Dhanekula Institute of Engineering & Technology, Ganguru, AP.*

Abstract - *Data Security in Cloud is an evolving sub-domain of computer and network security. The Cloud utilizes third-party data centers model. One example of cloud platform as a service is DriveHQ. This Cloud supports many programming languages that are used for web application deployment model. One mandatory issue in cloud computing is data security, which can be managed using cryptographic methods. One possible way to encrypt the data is Advanced Encryption Standard. In this publication, we apply DriveHQ as a cloud platform, after that we implement AES for data security in DriveHQ. The performance validation shows that AES can be used for data security. Apart from that, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.*

KeyWords: *Security, DriveHQ, AES, Cloud, Cryptography*

1. INTRODUCTION

Computation on Cloud can be implemented using various architectures. DriveHQ is a cloud platform as a service (PaaS). DriveHQ supports various programming languages. DriveHQ supports the development of cloud platform because it is free. Although it is free, it can also integrate with data services.

Nowadays, cloud computing serves as the solution for various problems faced by companies, because cloud technology has advantages such as flexibility, accessibility, and capacity compared to traditional online computing or storage method. Cloud platform has four deployment models for architecture solutions, which are private, community, public, and hybrid [1].

There are several security concerns associated with cloud computing. The issues are divided into two categories. **Firstly, a security issues by cloud providers. Secondly, security issues faced by their customers. They put data in the cloud and entrust the provider. That is why data security on cloud computing is needed.** Data security is a major issue in cloud computing to decrease the risk. These risks are generally associated with open, shared upload, and distributed environments [2].

DriveHQ consumers store data in a database application. It separates access control per application. Each database to connect needs to have a unique user and a password. The database in DriveHQ cloud uses MYSQL. Information in Cloud can be encrypted by the customer's applications to satisfy the security requirements. A famous and most secure encryption algorithm is Advanced Encryption Standard (AES). it is a symmetric block cipher with block size variation of 64 to 256 bits

2. RELATED WORK

Cloud computing has remarkably impacted every part of our human life and business forms. [3] Discussed approach and encryption technique also the implementation that approach. To enhanced data security and privacy, researcher combines AES 256 (Advanced Encryption Standard), IDA (Information Dispersal Algorithm) and SHA 512 (Secure Hash Algorithm). During the process encoding, the original data is encrypted using AES 256 algorithm, encryption generated is randomly by IT manager. Then the encrypted file is divided into several separate files. During the decoding process, verification stages are observed first. Further , reconstruct the data which is encrypted using IDA, then again convert original data using AES 256 to get original data. The result shows, average execution time higher when decoding time process is verification 1.453. Encoding results are encoding process depends on the value of (m, n), when the threshold is large, the verification time decrease and the reconstruction time increase. Otherwise, the threshold is small, the verification time increase and the reconstruction time decrease. [4] Also do research about security in cloud computing using AES & DES. Shows advantages and disadvantage AES and DES. In the experiment, the research implemented the algorithm and show the results to justify the thought of security for cloud computing. Cloud computing is delineated as the set of resources or services offered through the internet to the users on their requirement by cloud providers. So there is an urgency to assure that data adjacent illegal access, modification or denial of service.

Most of the cloud computing service need high performance to put away data in the cloud. Storage security refers security data on storage media, which is can quick to recover. Data Security should be considered by software engineer in the phase of design in cloud storage service. Not only pay attention to data redundancy or isolation but consider the data security. Redundancy is a basic measure to secure data security. Then, Isolation is because particular

user data is stored on the same platform, to ensure inter-data independency. Security is also an key issue in Amazon Simple Storage Service. Bucket, Object, and Key are the three S3 storage systems on Amazon[5]. Not only the data storage security but also consider the network transmission protocol. To ensure the safety product, protocol encryption plays a major role in protecting data when transmission. The most usual network security issue is the Secure Transmission Protocol and [6]Also discussed, the security of the data in cloud computing. Examine detailed method to ensure the maximum of protected data for reducing risk and threat. Data has two threats to the security of the cloud, there are when data on rest that is data storage in the cloud and data transmission which is data in or out from the cloud. Confidentiality and integrity of data are the base of data protection mechanisms, procedures, and processes. Data security techniques at rest and when transit data may be different. Example, the encryption key for data on transit over shorted live, while for data in rest, data key can be retained for the longer time. This study provides an overview of block ciphers, stream ciphers and hash functions used to encrypt data in cloud whether it is at rest or in transit.

3. SECURITY ALGORITHMS

Advanced Encryption Standard (AES) algorithm not only for security but also great speed. AES is the current standard for the encryption of secret key . AES is a symmetric key algorithm. It is having various chippers with different keys and the block size. In this plaintext is encrypted with the help of AES and then the ciphertext which we have got will again encrypt likewise there will be various round like the AES algorithm includes 10, 12 and 14 round with 128, 192, and 256 key bits. As there are various rounds in this algorithm the plaintext is encrypted many times and this helps the data to have the security [7].

AES is one the most efficient symmetric algorithm. The Advantages It provides strong security from attackers. Disadvantages are a major drawback is that its clouds not withstand the attacks like Brute Force, Linear Crypt Analysis

because during its design was not invented. In this paper, we have focused on AES 128 for making encryption of data. AES algorithm has four steps [8] :

3.1 Substitute Bytes

In this step, each byte of input data is replaced by another byte from the substitution table (S-box).

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 1. Substitute box (S-box) [9]

In the SubByte step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$

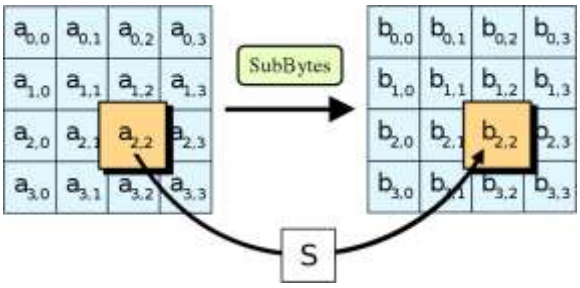

Figure 2. Sub Byte

3.2 Shift Rows

In the shiftRows, the byte in each of the row in the state is shifted cyclically to the left. The number of places shifted for each row is different for each byte.

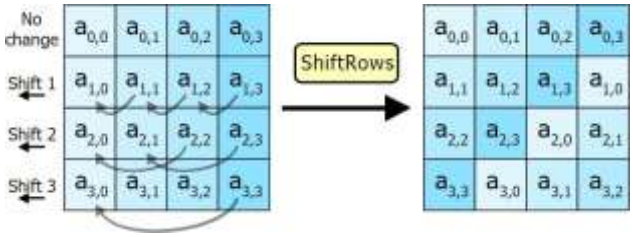

Figure 3. Shifting Rows

3.3 Mixing Columns

In this Mix columns each column represented in the state will be multiplied by a fixed polynomial.

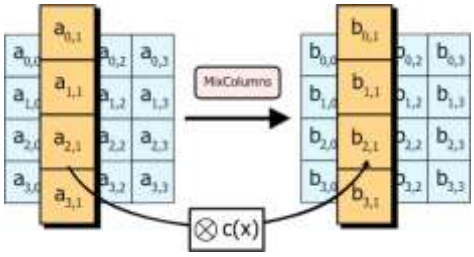

Figure 4. MixColumn

3.4 The AddRoundKey

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using XOR operation .

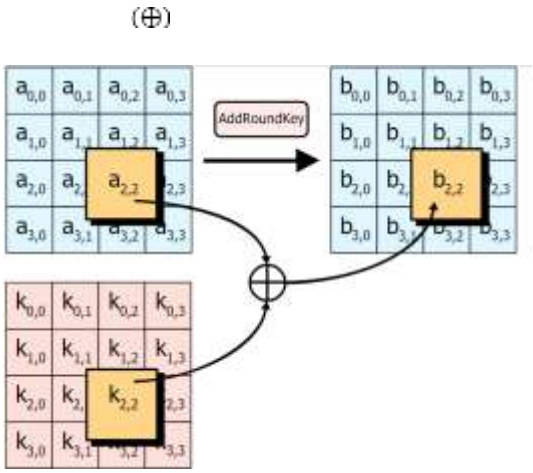

Figure 5. Adding Round Key.

4. DriveHQ Cloud

DriveHQ is the first Cloud IT service provider. Since 2003, It created a long list of Enterprise Cloud features.

Features:

Figure 6. Features of DriveHQ

- ✓ Cloud File Sharing
- ✓ FTP, Email & web Hosting
- ✓ Folder Syncronisation
- ✓ Drop Box Folder
- ✓ Cloud file storage
- ✓ Data Protection etc..

PERFORMANCE EVALUATION

Here, we will evaluate the performance of the data security under drivehq cloud.

It shows the performance evaluation of AES, Data security,DriveHQ cloud.

network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.
Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security concerns associated with cloud computing. These issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility is shared. However, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.
To protect data in cloud computing we can use cryptography. Advanced Encryption Standard (AES) is one of the most frequently used and the most secure encryption algorithms available today. It is publicly accessible, and it is the cipher which the NSA uses for securing documents with the classification "top secret". Its story of success started in 1997, when NIST (National Institute of Standards and Technology) started officially looking for a successor to the aging encryption standard DES. An algorithm named "Rijndael", developed by the Belgian cryptographists Daemen and Rijmen, excelled in security as well as in performance and flexibility.
In this paper, we will discuss about implementation security cloud using AES. For cloud we use heroku cloud. Heroku is a cloud

Figure .7 Plaintext

Figure 7 shows the plain text which we will encrypt. The file extension is .txt and its size is 4 kB etc.

The files will be encrypted using AES cryptography.

Figure.8 Cipher text

Figure 8 shows the result of encrypted data using AES.

With the evaluation and testing, we also calculate the delay in order to ensure data security. In real cloud platform which has many users, the flow of data will become at-most, which will have an effect on the system. In a real time, many factors could cause delay, e.g the network speed, file size etc., which will cause congestion and delay.

When the file is uploaded, it is initially split into different blocks before encryption. The size of each block depends on the file size. Delay metric is calculated as the sum of delay during the block-wise upload to a different location in the cloud [10].

$$Delay = T_s - T_b$$

Where T_s refer to Time after a successful load,

T_b refer to Time before load.

Calculation of delay is done by recording the encryption time for different files with a size ranging from 3000 kB to 15000 kB. The delay calculation is shown in Figure 9.

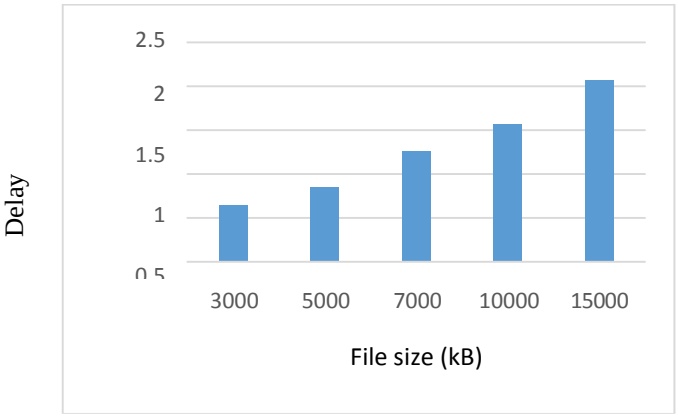

Figure 9. Delay calculation

5. CONCLUSION

In this publication, We had introduced Data Security Through AES under DriveHQ cloud. We implement this project by deploying driveHQ as a cloud through following various steps. After that we develop a web application for data security in which AES is used. Further the performance evaluation shown that AES can be used for Security of data and the delay calculation results shows that larger files take larger time for encryption.

6. REFERENCES

[1] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[2] L. Kacha and Abdelhafi Zitouni, “An Overview on Data Security in Cloud Computing,” Cybern. Approaches Intell. Syst., vol. 661, pp. 250–261, 2017.

[3] J. R. N. Sighom, P. Zhang, and L. You, “Security Enhancement for Data Migration in the Cloud,” Secur. Enhanc. Data Migr. Cloud, vol. 9, no. 23, pp. 1–13, 2017.

[4] S. Kumari, Princy, Reema, and S. Kumari, “Security in Cloud Computing using AES & DES,” Int. J. Recent Innov. Trends Comput. Commun., vol. 5, no. 4, pp. 194–200, 2017.

[5] D. Meng, “Data security in cloud computing,” in Computer Science & Education (ICCSE), 2013 8th International Conference on, 2013, pp. 810–813.

[6] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, “Data Security in Cloud Computing,” in Future Generation Communication Technologies (FGCT), 2016, pp. 55–59.

[7] A.Singh, P. Gupta, R. Lonare, RahulKrSharma, and N. A. Ghodichor, “Data Security in Cloud

Computing," Int. J. Emerg. Trends Eng. Manag. Res., vol. 3, no. 2, pp. 1–5, 2017.

[8] M. Usman and U. Akram, "Ensuring Data Security by AES for Global Software Development in Cloud Computing," in IT Convergence and Security (ICITCS), 2014 International Conference on, 2014, pp. 1–7.

[9] S. Trenholme, "The AES encryption algorithm," 2010.

[10] Babitha.M.P and K. R. R. Babu, "Secure Cloud Storage Using AES Encryption," in International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, pp. 859– 864.