EasyChair Preprint

№ 2615

Data Privacy Preservation Using AES-GCM Encryption in HEROKU Cloud

Prasenjit Kumar Das, Nidul Sinha and B. Annappa

February 9, 2020

DATA PRIVACY PRESERVATION USING AES-GCM ENCRYPTION IN HEROKU CLOUD

Prasenjit Kumar Das[1]
Department of CSE
NIT Silchar
Silchar, India
prasenjitdas139@gmail.com

Dr Nidul Sinha[2]
Department of EE
NIT Silchar
Silchar, India
nidul.sinha@gmail.com

Dr.Annappa[3]
Department of CSE
NITK Surathkal
Surathkal, India
annapa@gmail.com

***Abstract*— The increasing popularity of cloud data storage and its ever-rising versatility, shows that cloud computing is one of the most widely excepted phenomena. It not only helps with powerful computing facilities but also reduce a huge amount of computational cost. And with such high demand for storage has raised the growth of the cloud service industry that provides an affordable, easy-to-use and remotely-accessible services. But like every other emerging technology it carries some inherent security risks associated and cloud storage is no exception. The prime reason behind it is that users have to blindly trust the third parties while storing the useful information, which may not work in the best of interest. Hence, to ensure the privacy of sensitive information is primarily important for any public, third-party cloud. In this paper, we mainly focus on proposing a secure cloud framework with encrypting sensitive data's using AES-GCM cryptographic techniques in HEROKU cloud platform. Here we tried to implement Heroku as a cloud computing platform, used the AES-GCM algorithm and evaluate the performance of the said algorithm. Moreover ,analyses the performance of AES/GCM execution time with respect to given inputs of data.**

Keywords— **Cloud security, Encryption, Heroku, Public Cloud, AES-GCM**

I. INTRODUCTION

Cloud computing is a an important paradigm for hosting clusters of data and delivering different services over a network or the Internet [1]. Data is a vital for any organization. And it could be in any forms, i.e. numbers, words, images etc. and such digital data collection grows exponentially each year. As sensitive data generated and stored by individuals and organizations is rapidly increasing overtime the security are of major concern in cloud. Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security [2]. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Security is one of the key requirements to enable privacy. Security is often a deciding factor when choosing a public cloud provider. Every cloud service provider works the Internet, moving within infrastructure, or stored on servers. Every organization employs various security measures to ensure the authenticity, integrity, and privacy of user's data. Authentication verifies the source of data, either a human or a process, and destination.
Integrity: it make sure that data send receives at its destination unchanged. And to ensure the authenticity and the integrity of data stored, encryption is one of the important method[3].
Encryption: it is process making our data unreadable so that it cannot be accessed by any unauthorized users .The encryption algorithms used are public, but the key required for decrypting the cipher text is always remain private. Encryption can be used to protect data in three states.

i) Encryption at rest protects our data's from unauthorized access or data exfiltration by encrypting data while stored.

ii) Encryption in transit protects our data's while it moves between server and the cloud provider or between two services. And such protection are mainly achieved by using encryption of the data before transmission and then authenticating the endpoints. And at the other end on the data arrival it decrypts and verifies it.

iii) *Encryption in use*: protects our data when our data is being used by servers to run computations.

In this paper we mainly proposed a security architecture and implement AES/GCM algorithm in Heroku Cloud that acts as platform.

II. LITERATURE REVIEW

In paper [4] discussed various existing security issues in cloud and proposed a new method for data security using AES algorithm. Here the authors evaluated the performance along with delay evaluation. In paper [5] discussed various cloud features along with the associated security issues that are originated from various distributed, public nature of cloud. The authors also discussed various possible counter measure to mitigate such security threats. The authors in paper [6] provide solution of data with Encryptions and focuses on mathematical and logical solutions of RES. The pa-per also presented that Encryption may be one of the solutions to secure data in cloud and remove its vulnerability. In paper [7] reviews the risk management method and framework of cloud computing. It also reviews the framework of cloud computing and its respective strength and its limitations. In cloud security integrity is one of essential security goals that need to be ensured and in paper [8] the authors studied various issues that can ensure the data integrity in cloud computing. And to verify that in case of dynamic data, it used a third party auditor (TPA) that improved the Proof of Retrievability (PoR) model by manipulating Merkle Hash Tree (MHT) for block tag authentication. The researchers in the paper [9] has done a comparative study between different encryption methods-AES, DES and RSA. And based on analysis of simulation time for encryption and decryption of data it proved that AES algorithm performed better than DES and RSA. In paper[10] the authors tried to demonstrate the security issues related to IAAS and demonstrated how to improve IAAS CSP confidentiality and integrity. Data security being outmost concern of the owner and to mitigate such vulnerabilities the researchers in paper[11] reviewed different security techniques and challenges from both software and hardware aspects. Here they aims at enhancing the security and privacy issues for the real time cloud environment.

III.PROPOSED SECURITY ARCHITECTURE

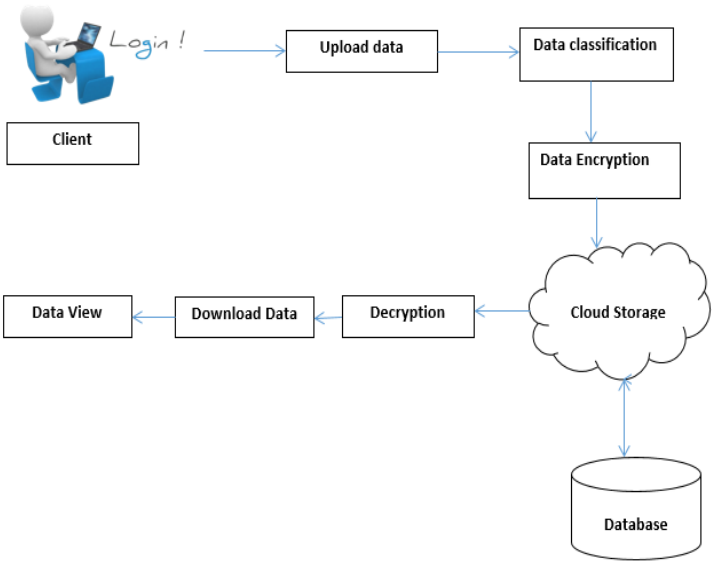

Figure1: Proposed Cloud Architecture

The proposed approach can be broadly divided into **two Phases**: Data Classification and Data Encryption. In this paper we mainly focused on the data encryption part which we have done by implementing the AES/GCM under HEROKU cloud. The overall description of the proposed architecture is discussed below:

Phase 1: Data Classification

In the data classification part the client data is being classified based on several parameters depending on the type of information. Data Classification is the process that defines various data levels and a level of sensitivity to it. It is an important activity at various stages as data's is being created, modified, stored, or transmitted. The classification of the data determines the extent to which the data needs to be secured according to its importance. Data classification is done based on the various aspects. Here, we mainly focus on the encryption of data's stored in details.

Phase 2: Data Encryption

Encryption module will encrypt the file using symmetric Key (secret key). For encryption process the algorithm used will be Advance Encryption Standard /Galois Counter Mode (AES/GCM). The reason for selecting AES/GSM is because it can make full use of parallel processing and GCM is an authentication encryption mode of operation, it is composed of two separate functions: one for encryption (AES-CTR) and the other for authentication (GMAC). It fills this need, whereas no other proposed mode satisfy the same criteria. Moreover it accepts initialization vectors of arbitrary length, which makes it easier for applications to meet the requirement that all Initialization Vectors(IV) will be distinct. Therefore it is able of acting as a stand-alone MAC, authenticating messages when there is no data to encrypt, with no modifications.
GCM basically has two operations, firstly authenticated encryption and decryption respectively. The authenticated encryption operation has four inputs, each of which is a bit string: K that represents secret Key, IV that stands for initialization vector which can have any number between 1 to 264, P that represents plaintext and lastly the Additional authenticated data(AAD) that have number of bits between 0 to 264[13]. Resultant there are two outputs mainly C that represents cipher text whose length is exactly the same with plain text P and T , the authenticated tag whose length can be any value between 1 and 128. The length is basically denoted by t. The authenticated decryption process mainly have five operations namely K,IV,C,A and T. And it has only a single output either P the plaintext or FAIL that signifies that inputs are not authenticated. Mathematically it is represented as follows:

$$H = E(K, O^{128})$$

$$\boldsymbol{Y_0} = \begin{cases} \mathbf{IV}||\mathbf{O^{31}}\ \mathbf{1} & \textbf{if len(IV)} = \mathbf{96} \\ \mathbf{GHASH(H, \{\}, IV)} & \textbf{Otherwise} \end{cases}$$

$$Y_i = incr(Y_{i-1}) for\ i = 1, \ldots, n$$

$$C_i = P_i \oplus E(K, Y_i) for\ i = 1, \ldots n-1$$

$$C_n^* = P_n^* \oplus MSB\big(E(K, Y_n)\big)$$

$$T = MSB_t\big(GHASH(H, A, C) \oplus E(K, Y_0)\big)$$

The encryption process is illustrated in figure 3 which shows successive counter values are then generated using the function incr(), which treats the rightmost 32 bits of its argument as a nonnegative integer with the least significant bit on the right, and increments this value modulo 232.

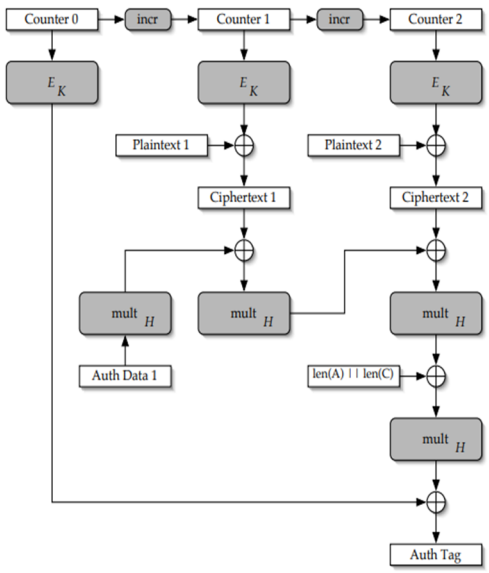

Figure 3: The authenticated encryption operation.

Only a single block of additional authenticated data and two blocks of plaintext is shown here for understanding.

AES/ GCM Decryption:

The authenticated decryption operation is almost similar to the encrypt operation, but with the reverse order of the hash step and encrypt step .More precisely, it is defined by the following equations:

$$H = E(K, O^{128})$$

$$Y_0 = \begin{cases} \mathbf{IV}||\mathbf{O^{31}}\ \mathbf{1} & \textbf{if len(IV)} = \mathbf{96} \\ \mathbf{GHASH(H, \{\}, IV)\ Otherwise} \end{cases}$$

$$T' = \mathrm{MSB}_t\big(\mathrm{GHASH}(H, A, C) \oplus E(K, Y_0)\big)$$

$$Y_i = incr(Y_{i-1}) for\ i = 1, \ldots, n$$

$$P_i = C_i \oplus E(K, Y_i) for\ i = 1, \ldots n-1$$

$$P_n^* = C_n^* \oplus \mathrm{MSB}\big(E(K, Y_n)\big)$$

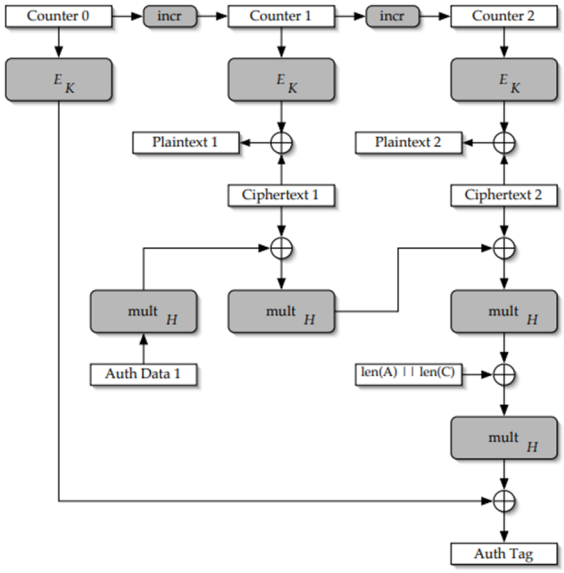

Figure 4: The authenticated decryption operation

After decryption operation the tag T' that is compared to the tag T associated with the cipher text C. If the two tags match , then the cipher text is returned. Otherwise, the special symbol FAIL is returned.

Here in our our work we used Heroku Cloud, is one of the leading provider of PASS which is almost alternative to PASS. Its platform provide abstract computing environments called dynos. Heroku, as a cloud platform as a service (PaaS), supports some programming languages like Java, Python, PHP, Ruby, Go, Scala and Conjure. Developed in 2007 HEROKU is one of the most commonly used cloud platforms

System Requirement:

The architecture of the cloud must be properly design and attractive. It must allow for efficient access to personal resources, proper installation of physical infrastructure. To implement our proposed architecture we have the following system requirements which is specified in the table below .Here the implementation is done by using Heroku cloud that act as platform. Deployment is done by JAVA application. Command Line Interface (CLI) is install for managing different applications, stipulation add-ons etc.

Table I: System Requirements

HARDWARE	Intel (R) Core (TM) i7-4770 CPU Memory 4 GB System type 64 bits
SOFTWARE	OS: Windows 10 Cloud: HEROKU Local Host: LARAGON Languages: JAVA

IV. EXPERIMENTAL ANALYSIS

The implementation of results in this section highlights the time of execution in encryption and in decryption of files with different sizes. Our application is developed in Java9 and as well as implemented on HEROKU Cloud. The result obtained in table II shows the performance of AES/GCM with respect to modes of operations. The figure 6 shows the graphical representation of the given results.

TABLE II : Comparative Table of Encryption Time among mode

Input (in MBs)	ECB	CBC	CFB	OFB	GCM
4	0.45	0.56	2.29	1.47	0.40
10	0.96	1.06	4.34	2.3	0.92
32	3.67	2.78	6.9	3.89	3.20
43	3.71	3.72	12.10	5.27	3.50
88	8.38	7.72	14.99	8.35	8.10
177	17.93	14.93	15.89	14.69	17.80
350	39.10	47.98	1:14.26	58.91	38.78
450	46.12	50.01	196.26	63.13	45.08
490	53.79	51.36	228.6	132.24	52.10
1600(1.61GB)	162.25	166.22	785.86	745.41	160.45
Average Time	33.36	34.63	135.94	103.56	32.13

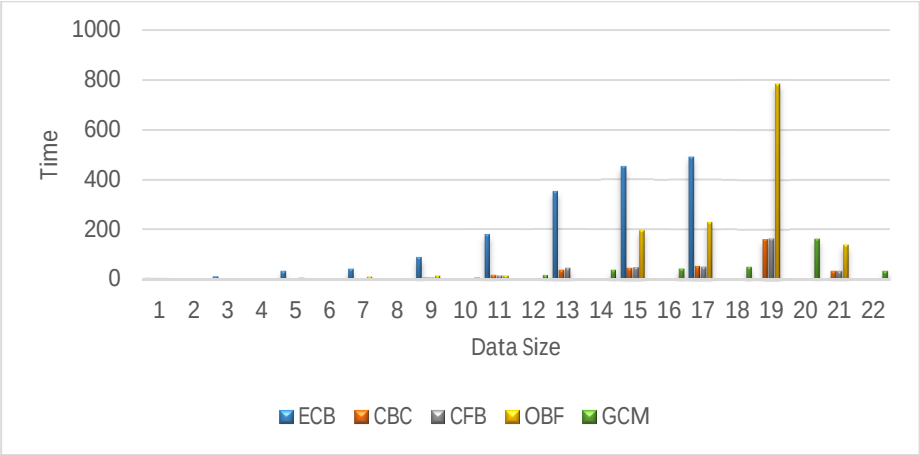

Figure 5: Graphical representaion of results

Next we perform the encryption algorithm under Heroku Cloud using AES/GCM algorithm and it is found that the files uploaded are securely encrypted before being and stored in the database. Moreover we calculate delay which is considered to be the prime for evaluating QoS of any system. In real cloud environment wit increase number of users and high size of data delays occurred. Here we have calculated the delay while uploading and downloading files with different sizes as shown in the figure below:

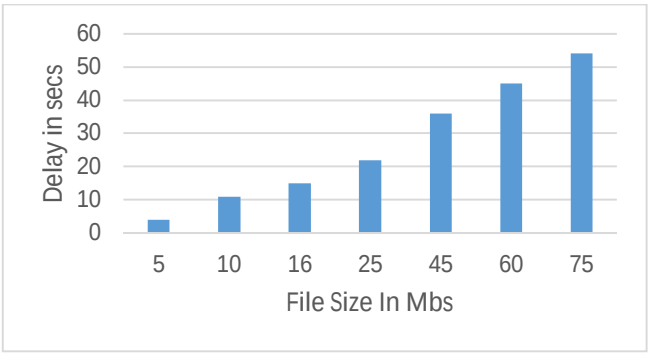

Figure 6: Delay occur during uploading files of different size

VI.CONCLUSION

In this paper, work has been done in providing an advanced security architecture with use of AES/GCM algorithm securing user's data in open cloud. Here, AES/GCM cryptographic algorithm is used as it provides more confidentiality and integrity of data. And, it has been proved that the encryption time taken is less compared to other modes of AES operations. Moreover, the encryption algorithm was implemented under HEROKU cloud platform and the performance of the proposed approach was analyzed on the basis of delay. From this particular delay evaluation it has been observed that with the increase in input size of data's the delay time got increased. Future work proposes a new intelligent method for secure data storage with effective proper classification of data's.

REFERENCES

[1] Agarwal, S. Siddharth, and P. Bansal. "Evolution of Cloud Computing and Related Security Concerns." In: Symposium on Colossal Data Analysis and Networking (CDAN) (2016).

[2] Torry Harris. Cloud Computing- An Overview.

[3] Y.Chen,R Sion, "On Securing untrusted clouds with cryptography" Proceedings of the 9th Annual ACM workshop on privacy in the electronic society, p.p 108-114

[4] Ashish singh, kakali Chatterjee,"Cloud security issues and challenges: A Survey" Journal of Network and Computer Applications, Elsevier, pp 88-115, vol 79,2017.

[5] Babitha M.P, K.R Ramesh Babu ." Secure Cloud Storage Using AES Encryption "International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (I²IT), Pune, 2016.

[6] Vigya Dubey and Pranjal Agarwal. "Cloud Com-puting and Data Management." Symposium on Colossal DataAnalysis and Networking (CDAN) 2016.

[7] Temesgen Kitaw Damenu and Chitra Bala. "Cloud Security Risk Management." 9th International Conference on Next Generation Mobile Applications, Services and Technologies 2015.

[8] Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in CloudComputing", IEEE Systems Journal, Vol.9, No.1, August 2015.

[9] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol.13, Iss. 15, Vol. 1, 2013.

[10] Dan Gonzales et.al**."**Cloud Trust- A Security assessment Model for IAAS",IEEE Transactions on Cloud Computing, Vol 5, No.3 ,2017.

[11] Y Sun et.al ," Data Security and Privacy in Cloud Computing:", Journal of Distributed Sensor Networks , SAGE, 2015.

[12] Heroku, "Heroku, " https://www.heroku.com/home, 2017.[Online]Availablehttps://www.heroku.com/home

[13] D. Hyseni, B. Cico, and I. Shabani. " The proposed model for security in the cloud, controlled by the end user." 4th Mediterranean conference on embedded Computing, pp. 81 –84,2015.

[14] Bastien Confais, Adrien Lebre, and Benoit Par-rein. "Performance Analysis of Object Store Sys-tems in a Fog/Edge Computing Infrastructures.**",** Transactions On Large-Scale Data- and Knowledge-Centered Systems XXXIII pp. 294-301,2016.

[15] Prasenjit Kumar Das; Arka Pratim Mandal; Nidul Sinha; Annappa B," Data Privacy Preservation based on Multitenant Isolation in Cloud ", International Conference on Computational Intelligence & IoT (ICCIIoT), 2018 (Elsevier)