Pranayanath Reddy Anantula *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 15-21 **ISSN: 2321-8363**
Impact Factor: 5.515

PROTECTING DATA USING PLATFORM ENCRYPTION IN CLOUD

Pranayanath Reddy Anantula[1], Dr. G Manoj Someswar[2]

[1]Ph.D Research Scholar, Department of CSE, Pacific University, Udaipur, Rajasthan, India
[2]Principal & Professor, Department of CSE, NRI Institute of Technology(under JNTU-Hyderabad), Kothur, Greater Hyderabad, Telangana State, India

Abstract

Cloud computing has became a change over for all the enterprise applications. Everyone is adapting cloud and its services to operate their applications effectively, efficiently with minimum cost to company. The major concern for any organization is how data been handled in storing, processing and managing it in cloud. As data is storage in shared memory with multiple tenants, data must be protected from begin leaked and accessed by the other tenants. The classical approach is encrypting data before storing it into cloud. Similarly to access the data, we need to decrypt it before displaying to the user. This process takes more time in verification of key while doing encryption and decryption for each and every transaction. To reduce the time and add extra layer of protection we are using platform encryption process. In this paper we have proposed a platform encryption process that includes unique tenant and master secret keys. We combined these secrets to create unique encryption key. The key is used to encrypt and decrypt data on cloud.

Keywords: Hardware Security Model, Key Derivation Function, Master Secret, Platform Encryption, Tenant Secret.

1. Introduction

Cloud computing is taking over to the traditional computing. Adaption cloud computing has grown exponentially due to various services provided by the cloud service providers which make the management of application easy at minimum cost. Organizations are migrating their existing and also developing new applications using cloud based technology. The most important aspect a customer looks before adapting to cloud is how security and privacy of data is handled and maintained. Privacy of information through authentication is being considered as vital task. Privacy and security can be provided using user authentication with passwords or digital certificates (D Jayalatchumy et al., 2010). Trust of cloud services relies in how

privacy and security of sensitive information is addressed and handled in the cloud. The major problem arises due to multi tenancy framework; the chances of cross-data exchange may exist because of sharing storage device. This raises the point of privacy and security of data when storing the data in the cloud environment.

Privacy, legal compliances, user trust need to be considered at every phase of design when we are dealing with in cloud computing services (W Jian et al., 2009). Security means protecting organization data from intruders. Any kind of security breach is not acceptable in cloud environment because even a small breach may lead to a great loss to the cloud vendors and also to customer business. Security and Privacy control allows the person to maintain a degree of intimacy (Wang B et al., 2012).

The growth of cloud computing depends on the data security and privacy. These two are considered major issues that hamper the growth of cloud computing because data is considered at most critical and generation of data is growing in exponential way. Various attempts have been made in the past to safeguard the privacy of the individual or agency trying to utilize the services being provided by the cloud (Syed & Mohammad, 2012). Users must guarantee for feeling that security and privacy of data has been ensured in cloud environment (Syed & Mohammad, 2012).

File encryption key is generally saved with plaintext in the memory in the current solutions. To protect the sensitive data is always a key challenge especially we are now in the data explosion age. Some modern file systems have supported the build-in encryption functionality, e.g., Linux Ext4, Chrome OS, and Windows Encrypting File System (EFS).

To protect sensitive data we can use Encryption file system at storage media. The files are encrypted using File Encryption Key (FEK) when they are written to disk. However, in the encryption file systems, the FEK is normally used as plaintext in memory. This will be a prone to security vulnerability such as cold boot attack. The encryption key is stolen using cold boot attacks; they use the key for decrypting the files.

The challenge in securing data in cloud is to obtain flexible means and able to deal with the intensive computation needed by the cryptography algorithms.

Before applying security to organization data, we need to identify the most likely risks and threats to organization data. This help in distinguish data that needs encryption and from data that doesn't required. This will save the processing time.

The following points need to be considered.

1. Define a threat model: Walk through an existing threat modeling and exercise them on organization data to identify the threats that may affect the organization. Outcomes of it will help in creating data classification scheme, which helps to decide what data to encrypt.
2. Encrypt only vital data: Entire organization data is not sensitive. Encrypting entire data will impacts functionality and performance of system. Focus on data that requires encryption and which meet security, and privacy requirements.
3. Data Classification scheme: Identify the scheme to classify the data at early stage. Work closely with technology experts to define requirements that meet security, privacy and compliance.
4. Risk Measurements: Measure the risks against security in critical functionalities and periodically challenge the assumption to take proactive measures to deal with the risks that may arise.
5. Strategy to handle keys: Create strategy how to implement, backing up and archiving keys and data.
6. Encrypt data using the latest key.

In this paper we discuss data security using Platform Encryption. It gives a new layer of security for Organizations in preserving critical functionality in cloud. Organizations can handle critical data with confident and also comply with security and privacy requirements.

Advanced HSM based key derivation system is used to encrypt the data. It will assure that even other lines of defenses are compromised data will be secure. The key used to encrypt data is never stored or shared across organizations. Instead, it is derived dynamically on demand at runtime using master secret and organization-specific tenant secret. To reduce the processing time it would be better to cache the latest key on an application server.

2. Related Work

Technology is a key of innovation in any aspect of this modern era. Whichever technology it may be protecting the data becomes the basic functionality and it is the most important asset. Many encryption algorithms are available in market and most of them are used in information security. Encryption can provide information security across platform.

At each security levels various techniques or algorithms are implemented, as security levels increases the processing time and algorithm complexity also increasing. This is the major cause of setback in processing speed and efficiency of the encryption system.

There exist various cryptography algorithms in market which are optimal and efficient, here we used the combination of existing algorithms, and developed a framework for encrypting and decrypting data at runtime in cloud environment.

The Cost of Data Breach Study found the average consolidated total cost of a data breach is $4 million in 2016. As per CIA, Transactions made over network should be confidential, and also it should ensure data authentication, accountability, integrity and availability (Tingyuan et al., 2010).

(Kurniawan et al., 2016) had discussed Double chaining algorithm and compared which encryption algorithm is efficient using various parameters. Parameters considered such as speed, space, and complexity of algorithms.

(Wenqian et al., 2016) discussed in their paper proposed encryption systems based on HSM for a Linux operating system. They have also shown how HSM can provide extra security from different attacks such as cold boot attack etc.

Microsoft Corporation provides technique to protect sensitive data at storage media. Files are encrypted with file encryption key (FEK) before the file is written on to the storage media.

(Vaidehi & Rabi, 2014) had discussed how AES, IV and CBC modes can be used to provide high security for data. More complex modes of operations are combined with the data of previous ciphered message and combining IV to it making each ciphered message a unique one.

(Robert & Oklahoma, 2015) has proposed a Key derivation function which takes a passphrase and a picture as input to generate a unique key. The function takes randomly some pixels from picture and converts them in to binary strings that are used in generating keys.

(Thambiraja et al., 2012) the strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how these are implemented together.

3. Key Terms

Before going into the process we need to known the terms used in Platform encryption

Tenant Secret

It is an organization-specific secret key. Administrator can rotates a key and generate a new tenant secret key. Rotating Key is required to generate new tenet secret key. Before rotating the key we need to archive the active one for backup. The new key will be used for both encryption and decryption of data. For the data which was encrypted using Archived keys will be decrypted by only archived key, the data will be encrypted by new key when the old data is re-encrypted.

Master Secret

The master secret is a cloud service provider's key. The secret key keeps on changing for every major release of updates of cloud platform. The new key is encrypted using master wrapping key, before storing it on the file system it again encrypted with public key of the KDS's.

Master Wrapping Key

A symmetric key used as a master wrapping key to encrypting all the release keys and secrets bundle.

Initialization Vector (IV)

A random sequence used to encrypt data. It is used in deriving encryption key in combination of tenant secret and key derivation function.

Hardware Security Module (HSM)

It is used to derive data encryption keys and provide services in cryptography process and in key management.

Master HSM

It is a USB device used to generate random secrets for each release, and it is done in secure manner.

Key Derivation Function (KDF)

It generates a key by taking a pseudorandom number and password as inputs. There exists various KDF's such PBKDF2, which can be computationally expensive and too slow to be used in some systems. Although some technologies will be able to withstand lower usability or efficiency from certain implementations of slow KDFs, others may not; it is therefore necessary to choose the best key derivation function that meets security, usability, and efficiency requirements.

4. Platform Encryption Process

All Service providers need to generate master and tenant secrets by using HSM securely. The unique key is derived by using 1) PBKDF2 2) with HMAC-SHA-256, the master and tenant secrets acts as inputs.

When user submits data through UI, the application server looks for key in cache. The organization-specific data encryption key is kept in cache for faster access. If key is not cached, application servers retrieves

encrypted tenant secret from the database and forward it to key derivation server to derive the key. Then application server will encrypts the data and store in cloud storage.

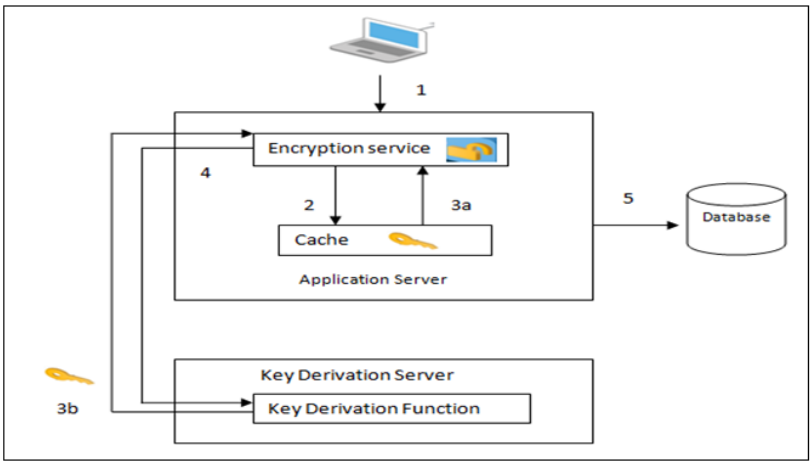

Figure 1: Platform Encryption Process Flow

The process flow is as follows.

1. When user wants to save data, metadata determines which data to encrypt.
2. Application server checks for encryption key in cached memory.
3. a) If key exist in cache, the application server retrieves the key
   b) If not, the server sends a request to a derivation server to generate key.
4. Application server on retrieving or deriving the key, it generates a random IV and data gets encrypted using 256-bit AES encryption.
5. The cipher text is saved in the database or file storage.

Data Encryption

The following are used in encrypting data and files.

- ✓ Symmetric key
- ✓ 256-bit AES algorithm with CBC mode (cipher block chaining)
- ✓ public-key cryptography standards- PKCS5, and
- ✓ Randomized 128-bit IV

The following table 1 shows some of the factures that are available in platform encryption when compared to Classic Encryption.

5. Manage Platform Encryption

We can generate, export, import, and destroy organization-specific keys; only authorized users are permitted to create keys. Similarly tenant secret key can be generate, rotate, export, destroy and re-import.

Generate a Tenant Secret

Controlling own tenant secret entails generating a Own Key(OK)-compatible certificate. In the event of unauthorized access to critical data, OK acts as an extra layer of protection. The certificate used to encrypt the tenant secret is also use to derive org-specific data encryption key. The certificate can be a self-signed or

certificate-authority (CA) signed type certificate and including tenant key, private key, and size of the key, platform encryption key.

Table 1: Comparing Classic Encryption and Platform Encryption

Features	Classic Encryption	Platform Encryption
Encryption Algorithm	128-bit Advanced Encryption Standard (AES)	256-bit Advanced Encryption Standard (AES)
HSM-based Key Derivation	-	X
PCI-DSS L1 Compliance	X	X
Masking	X	X
Mask Types and Characters	X	-
Generate, Export, Import, and Destroy Keys	X	X
Encrypted Attachments, Files, and Content	-	X

We can generate tenant secret using external resources. We can use a random number or use crypto libraries or enterprise key management system or HSM.

The process of generating tenant secret keys is as follows
1. We need to generate a 256-bit tenant secret encrypted with a public RSA key
2. Wrap tenant secret with the public key from the OK-compatible certificate, specify the OAEP padding scheme.
3. Encode encrypted tenant secret to base64.

Rotate Encryption Keys
To control data encryption key we need to control the lifecycle of tenant secrets. To maintain the security, often we need to generate new tenant secret and archive the old one.

Back Up Tenant Secret
We need to maintain the backup of tenant secrets at regular interval or whenever a new tenant key is generated. The archived key will ensure continued data access to old data which has encrypted using archived key.
Destroy Tenant Secret
We need to double check before destroying the tenant secret because once we destroy it the data which was encrypted using it will not be accessible. If access to data is no longer needed, we can delete tenant secret.
The keys that are generated are not stored. Instead, they're derived on demand at runtime whenever a key is needed. The tenant secret is unique to organization, and we can control it.

6. Conclusion

Protecting and securing data is a vital functionality. Cloud providers can provide extra layer of security using platform encryption. In this platform encryption process, Tenant and master keys used in Data encryption and these keys are never stored or shared across organizations. Instead, they are generated at runtime on demand using master secret and tenant secret. The generated key is then cached on an application server. Caching of derived key will fasten the process of verification, encryption, and decryption services. It indirectly increases

the performance of the system. Creating tenant secret using OK provides an additional protection to tenant key. Key management is required to maintain the organization system protected and updated with the latest risks and threats.

References

[1] Daniar Heri Kurniawan , Rinaldi Munir, 2016. Double Chaining Algorithm: A secure symmetric-key encryption algorithm. *IEEE Conference on Advanced Informatics: Concepts, Theory and Application*.pp.1-6
[2] D Jayalatchumy, P Ramkumar, and D Kadhirvelu, 2010. Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm. *Third IEEE International Conference on Emerging Trends in Engineering and Technology*, pp. 456-461. DOI 10.1109/ICETET.2010.103.
[3] E. Thambiraja, G. Ramesh, R. Umarani, 2012. A Survey on Various Most Common Encryption Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*. vol. 2, no. 7, pp. 226-233.
[4] Ghada Farouk Naiem , Salwa Elramly , Bahaa Eldeen Hasan , Kaled Shehata, 2008. An efficient implementation of CBC mode Rijndeal AES on an FPGA. *Radio Science Conference*. pp. 1-8.
[5] Junyuan Wang, Weigang Li, Wenqian Yu, 2016. A study of HSM based key protection in encryption file system. *IEEE conference on Communications and Network Security*. pp. 352-353.
[6] M. Vaidehi , B. Justus Rabi, 2014. Design and analysis of AES-CBC mode for high security applications. *2nd International Conference on Current Trends in Engineering and Technology*. pp. :499- 502.
[7] Nie Tingyuan, Song Chuanwang, Zhi Xulong, 2010. Performance Evaluation of DES and Blowfish Algorithms. *IEEE International Conference on Biomedical Engineering and Computer Science*, pp. 1-4.
[8] Prerna Mahajan, Abhishek Sachdeva, 2013. A Study of Encryption Algorithms AES DES and RSA for Security. *Global Journal of Computer Science and Technology Network Web & Security*, vol 13(15), pp.15-22.
[9] Porter E. Coggins 2013. A pedagogical example of a stretched password-based key derivation function. *Journal of Computing Sciences in colleges*, Vol 28(4), pp. 125-131.
[10] Robert Grimes, Oklahoma J. F. Yao, 2015. Development of a novel key-derivation function for speed, security and simplicity in picture-passphrase encryption. *Journal of Computing Sciences*, ACM, Volume 31 (2), pp 194-200.
[11] Syed Mujib Rahaman, Mohammad Farhatullah, 2012. A framework for preserving privacy in cloud computing with user service dependent identity. *ICACCI '12: International Conference on Advances in Computing, Communications and Informatics*. ACM. pp 133-136.
[12] Syed M. R, and F Mohammad, 2012. PccP: A Model for Preserving Cloud Computing Privacy. *IEEE International Conference on Data Science & Engineering*. pp. 166- 170.
[13] W Jian, Y Wang, J Shuo and Le Jiajin, 2009. Providing Privacy Preserving in cloud computing. *IEEE International Conference on Test and Measurement*. vol 2, pp. 213–216.
[14] Wang B, Baochun Wang, H. L., 2012. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. *Fifth IEEE International Conference on Cloud Computing*. DOI 10.1109/CLOUD.2012.46. pp 295 – 302.
[15] Cost of Data Breach Study: Global Analysis, Available online at http://www-03.ibm.com/security/data-breach/. Accessed on April 15, 2017.
[16] How to back up the recovery agent Encrypting File System (EFS) private key in Windows, Available online at http://support.microsoft.com/kb/241201. Accessed on April 21, 2017.

A Brief Author Biography

Pranayanath Reddy Anantula, B.Tech, M.Tech,(Ph.D.) is a Research Scholar at Pacific University under the Guidance of Dr.G.Manoj Someswar. He did his M.Tech degree in Software Engineering and B.Tech degree in Computer Science and Information Technology. Presently, he is working as an Assistant Professor in CS Department at Alliance University, Bengaluru, Karnataka, India. His research interests include Cloud Computing, Software Engineering, Software Testing, and Database Management Systems.

Dr. G.Manoj Someswar B.Tech., M.S.(USA), M.C.A., Ph.D. is having over 30 years of relevant work experience in Academic Administration, General Administration, Academics, Teaching, Industry, Consultancy, Research and Software Development. At present, he is working as Director General & Scientist'G', Global Research Academy, Hyderabad, Telangana, India and utilizing his research skills, teaching skills, knowledge, experience and expertise to achieve the goals and objectives of the Research Organization in the fullest perspective. He has attended more than 100 national and international conferences, seminars and workshops both in India & Abroad. He has more than 250 research paper publications to his credit both in national and international journals. He is also having to his credit more than 100 research articles and paper presentations which are accepted in national and international conference proceedings both in India and Abroad. He received National Awards like Rajiv Gandhi Vidya Gold Medal Award for Excellence in the field of Education and Rashtriya Vidya Gaurav Gold Medal Award for Remarkable Achievements in the field of Education, National Award for Research Excellence, Sardar Patel International Award for Academic Leadership, and Distinguished Professor Award from Computer Society of India.

