International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Cloud Security: Providing security to the cloud using Decoy Technology and HMAC

Jui Matey[1], Ria Shetty[2], Arti Pandey[3], Prof. Rushikesh Nikam[4]

[1,2,3]Student, Dept. of Computer Engineering, New Horizon Institute of Technology and Management, Thane, Maharashtra, India
[4]Asst Prof, Dept. of Computer Engineering, New Horizon Institute of Technology and Management, Thane, Maharashtra, India

---

Abstract - *Deployment of two-factor authentication is a more powerful technique for security systems. Business decisions and processes are highly dependent on accurate and reliable data. If data gets tampered and the alterations go unnoticed, it could affect decisions and processes down the line. So if your data has to be transmitted over a network, especially one as perilous as the Internet, you have to take precautionary measures to preserve its integrity or at least know if it underwent unauthorized alterations. Many organisations are shifting their interest from traditional storage to cloud storage. As the data collected and hoarded in the cloud is accessible very easily it might also be effortlessly invaded by an attacker. Considering the amount of information that various sectors need to reserve in the present situation creates an obligation for protecting it. This paper focuses on the implementation of a two-factor authentication mechanism for data security. It emphasizes the use of two techniques namely Decoy Technology and HMAC. The systems are vulnerable if an outsider gets an entry without any obstacles. The first authentication factor consists of entering the user's password. The second authentication factor is entering a secret key, displayed on the screen, and also received via an email on the registered email id. A legitimate user will be guaranteed entry into the system only if he/she clears both authentications. If they fail to prove their identification they will be categorized as attackers and will receive a decoy file if by any chance they enter the system.*

Key Words: Cloud Computing, HMAC, Decoy Technology, data security, AES, SHA, MD5

1. INTRODUCTION

With the proliferation of online activity, more and more information is saved as data every day, meaning that more being stored in the cloud than ever before. Cloud computing [2] [3] means that instead of all the computer hardware and software you're using your desktop. It is provided to you as a service by another company and accessed over the Internet. Massive amount of data gets collected and hoarded in the cloud. This data is then accessible very easily which might also be effortlessly invaded by a third person and safety of the data is compromised within the cloud. If this third person turns out to be a cyber-criminal then they might invade the system with a reason to annihilate, embezzle or exploit an organisations vital information. Data that is stored online often holds private information – such as addresses, payment details and medical documentation – that becomes the target of cyber criminals. Security capabilities are put in place to combat cyber threats and vulnerabilities, ensuring data is not leaked which could endanger those whose private information has been released. Implementing security at such platforms is inevitable. Conventional approaches were not reliable for the data security as the key would be easily compromised. In this paper we discuss the proposed system built on public cloud where data is protected against data thefts using HMAC [7] and Decoy Technology [6].

1.1 HMAC

HMAC stands for Keyed-Hashing for Message Authentication [7] and is a hashing algorithm. HMAC message authentication algorithm comprises of cryptographic hash function and a secret cryptographic key.

The proposed system makes use of SHA-256 [19] as the cryptographic hash function and the users email id as a secret key. SHA-256 is a message-digest algorithm and is used to generate a fixed-size hash value for a given input. SHA-256 produces a 265- bit (32 bytes) hash value representing a hexadecimal number of 64 digits. The hashing algorithm generates only generates hash value, so these hashes are not reversible and cannot be decoded to the original text message. HMAC-SHA-256 is secure than HMAC- MD5, because HMAC-MD5 experiences collision vulnerabilities [15] even with MD5 as the underlying hash function.

1.2 Decoy Technology

Decoy technology [5] is an emerging field in cyber-security. Decoy data known as misinformation [6] for bogus information can be generated on demand and used for detecting unauthorized access to information. Serving decoys will confuse an attacker into believing they have filtrated useful information when they have not. This technology can be used to secure information on the cloud. Unlike the traditional approach that tends to block users seeking unauthorized access, this technology returns files that appear as legitimate.

Users can view and add their files, these files are stored alongside the user-id column in the database. User id is a unique non-zero id that a session key creates after successful registration, making them user-specific. Decoys for the same

files will be maintained by the admin in the database itself alongside an id value equal to zero.

User id of zero and non- zero values are associated with differentiating users and fake files respectively. After successful completion of the two-step authentication process, users are categorized as genuine users. They may wish to add or view files. For viewing a file they will have to download it and can view the contents of the file. For such legitimate users when they complete both authentication steps the user id matches with the user id in the database and true files can be directed to them. In case of an intruder, he will try to enter incorrect credentials, so the user id for such users will not match the ones already stored in the database because such a user does not exist. Under such circumstances, the son will be directed to decoy files. An email under the name of security will be immediately sent to the user whose data the intruder tried to breach.

2. Literature Survey

Cloud computing is the delivery of computing services like servers, storage, and computing services over the Internet. Organizations that offer these computing technologies are called cloud providers. These service providers support the idea of pay as you use. Customers are charged on an hourly basis. Depending on the type of data you're working with, you'll want to compare public, private, and hybrid clouds in terms of the different management levels. Following are the various types cloud [17].

1. Public Cloud – The resources are offered to the public with the help of the internet. Computing resources and services are accessible by every cloud user with every individual's data being hidden from other individuals.

2. Private Cloud – Every individual or organisation have a private cloud. Security is maximum here as others will require access permission to their cloud. Along with other cloud computing resources, private cloud also offers physical computing resources stored on-premise.

3. Hybrid Cloud – Hybrid offers mixed services offered by public and private clouds. It provides on-premise private cloud services and third-party public cloud services. Hybrid cloud services are considered powerful because they provide greater control over private data in business.

4. Community Cloud – A community cloud refers to a shared cloud computing environment. It is shared between organizations with a common goal or that fit into a specific professional and geographic community, etc.

Cloud computing services [18] fall into the following 3 categories: Software as a service (SaaS), Infrastructure as a service (IaaS), and Platform as a service (PaaS)

1. Software as a Service (SaaS): It provides you complete software and product managed and run by third party members. SaaS provides an end-user application, where the service users need not worry concerning the underlying infrastructure, maintenance, and working of the application. Users solely get to target a way to use these options for his or her use. Installing applications needed infrastructure and programs is not required as their services are obtainable over the internet.

2. Infrastructure as a Service (IaaS): These services offer online computing resources such as infrastructure for your application like raw compute, data storage space, and network organized. You pay only for the services allotted within the IaaS model. IaaS contains the essential building block of cloud IT and provides you with the highest level of flexibility and management control over your IT resources that a lot of IT departments and developers are aware of nowadays.

3. Platform as a Service (PaaS): They provide storage, networking, and virtualization services, that the organizations needn't worry concerning the management of underlying hardware and software package that successively permits organisations to simply target the deployment and management of applications. This will be very beneficial as cloud users don't have to worry about resource allocation, capacity planning, software maintenance, patching, or any of the other utility involved in running your application.

We used public cloud [17] for deployment using SaaS [18]. The resources are offered to the public with the help of the internet. Computing resources and services are accessible by every cloud user with every individual's data being hidden from other individuals. Saas is an acronym for Software as a Service, provides you complete software and product managed and run by third party members. SaaS provides an end-user application, where the service users need not worry concerning the underlying infrastructure, maintenance, and working of the application. Users solely get to target a way to use these options for his or her use. Installing applications needed infrastructure and programs is not required as their services are obtainable over the internet.

The fake files used to trick the attacker are decoy files. Decoy technology is an emerging field in cyber-security. Decoy data known as misinformation or bogus information can be generated on demand and used for detecting unauthorized access to information.

Decoys that are very much similar to a user's real data misguide the attacker from the sensitive information preventing data theft. Unlike the traditional approach that tends to block users seeking unauthorised access, a technology that returns fake files that appear as legitimate came into picture. It was used in various places when customer information seemed valuable, to defend against a third party who may gain illegitimate access to steal information. It can either be a human trying to get access to an organisations sensitive information or a malware program stationed in the personal system.

Decoy have certain features. First, it should be believable, and should appear authentic and trustworthy. Second, the decoy should be engaging enough to draw in the attention of the attacker and make him/her open the file. Third, the decoy ought to be differentiable so the legitimate user will

distinguish between real and decoy files. This technology can be used to secure information on the cloud.

User specific secret Key available at the time of second authentication is generated using HMAC. HMAC is Keyed-Hashing for Message Authentication. RFC 2104 and FIPS 198 NIST standard has issued HMAC. Secure file transfer protocols like FTPS use HMACs instead of just hash functions because MAC functions provide authenticity of the messages, whereas HMAC incorporates both data integrity, message authentication, and is very efficient. It is a particular type of MAC that consists of cryptographic hash function and a secret cryptographic key. HMAC can be pared with cryptographic hashes like SHA [19], MD5 [16], denoted as HMAC-MD5, HMAC-SHA1, or HMAC-SHA256. Participants involved in the message transmission process will receive HMACs rather than plain hashes. The hash functions are selected based on how strong an underlying cryptographic hash is to ensure maximum security in data transfer. HMAC-SHA-256 used in the model takes 32-bit word and generates a unique 256-bit hash value. A shared key is generated during the key exchange process and requires participation from both end-users. In our model we use the users email id.

AES is Advanced Encryption Algorithm, iterative and one of the widely perceived and applied symmetric key [12] algorithm. Issued in December 2011 by the National Institute of Standards and Technology (NIST). AES algorithm used for file encryption is AES-128. This algorithm inputs an equal-sized input block data and yielding an output of the same block size, 128-bit cipher text, and plain text respectively. An input key is also required by the algorithm. For users file encryption, user specific secret key is used, whereas for the encryption of decoy files a single unique key is used.

For the admin password MD5 is used, it is a Message Digest Algorithm [16]. Md5 was originally developed for authentication of digital signatures using cryptographic hash algorithms. MD5 takes an input of variable length and produces an output of 128-bit. In recent studies it was found that HMAC-MD5 was found vulnerable to the collision related vulnerabilities, in spite of underlying MD5 hash function. It is now intended to generate digital signatures, where a variable size file should be compressed securely

3. Proposed System

The proposed system aims on securing the vital information on the cloud by employing two-factor authentication [2]. The first factor involves the user login using correct login credentials. The second factor is entering the secret key generated using HMAC [7]. MD5 [14] will be used for admin login and AES for file encryption [11]. Following fig-1 shows the system architecture.

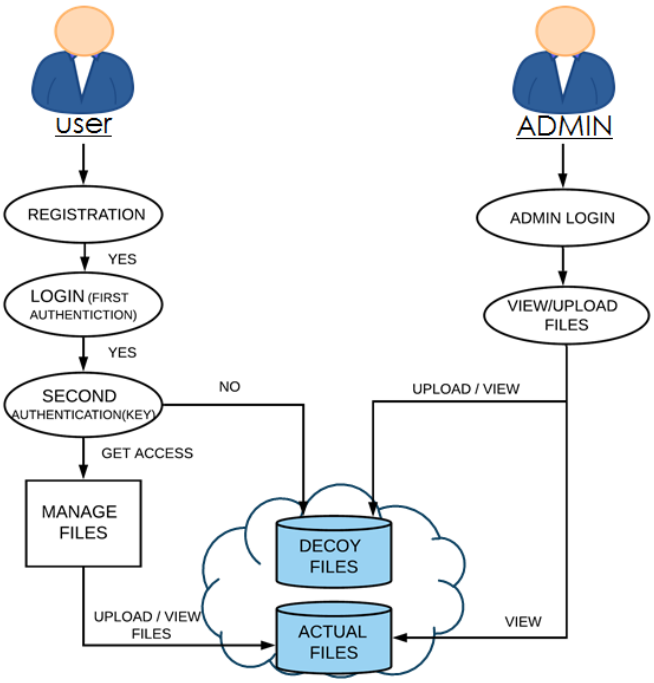

Fig -1: Architecture of system

3.1 User Module

1. User registration

In this module, the new user initially has to register themselves. The registration will comprise of certain personal credentials to create an account, the password can be any strong array of characters, numbers, or special characters.

2. User login

The user is prompted to enter their admissible email id and pw they submitted during the registration when they log in. At the time of log in a secret key, generated using HMAC and SHA-256 [19] will appear on their screen as a part of the second authentication. An electronic mail on users' email id will be sent containing this key and the user-created password. A new account with the registered email id will be set up on entering the secret key. Keys are email id specific, and the same will be required in the future to access the account.

3. User files

The interface is user friendly, once logged in the users can upload and their view files in their account. Uploaded files will be stored in the database below the user id. Files are encrypted using AES algorithm before storing it in the database. The key generated at the time of the second authentication [2] will be used for encryption, the key will differ from user to user this way even if the intruder attacks the database he won't be able to read the content of the files. The same key will be used for decryption. As we know these user ids are specific and will assist in redirecting the original files to legitimate users.

3.2 Admin module

1. Admin login

The program has default login credentials for the admin login, which uses MD5 for creating admin password [16]. Later the service providers or the organization can reset the admin's unique login credentials accordingly. Database, user files, and decoy files will be managed by the admin itself.

The essential content of the user's files won't be visible to the admin either, only the type, size and name of the file will be known.

When a user uploads a file, it gets stored in the database in the user id column, provided every user has a unique user id. The admin of the system will manage decoy files. Decoy of every user's file with the same name and scrambling content is being stationed on the database by the admin. Users who log in using correct credentials will get the real files as their user ids will match with id in the database. When an intruder tries to gain access to the files with a false password or key, their system generated ids will not match with the one in the database as they don't exist, thereby redirecting them to decoy files. At the same time, a security message will be sent to the same users at their registered email, of whom the intruder intended to steal data. Thus, ensuring data security [9] [5].

4. SYSTEM EVALUATION

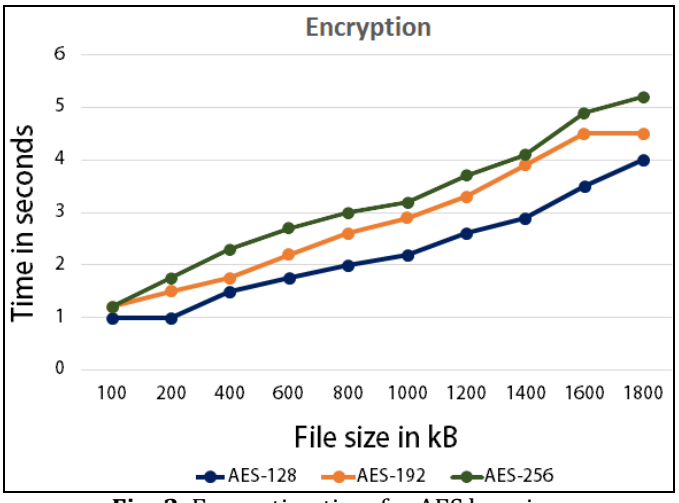

Fig -2: Encryption time for AES key sizes

Fig-2 illustrates the time of encryption for AES-128, AES -192, and AES-256, with various file sizes. In the above graph time taken for AES-128 takes 1 second, AES -192, and AES-256 takes 1.3 seconds respectively to encrypt 100 kB file. For a file size of 1000 kB AES-128, AES -192 and AES-256 takes 2.2, 2.8, 3.2 seconds respectively. Whereas for a file size of 1800 kB the algorithms take 4, 4.5, and 5.2 seconds respectively. As observed the time taken for encrypting increases proportionally with an increase to file size, with AES-128 taking the minimum and AES-256 taking the maximum time for encryption

Fig -3: Decryption time for AES key sizes

Fig-3 illustrates the time taken of decryption for AES-128, AES -192, and AES-256, with various file sizes. In the above graph time taken for AES-128, AES -192, and AES-256 to decrypt 100 kB file are 0.5, 1, 1.2 seconds respectively. For a file size of 1000 kB AES-128, AES -192 AND AES-256 it takes 2, 2.3 2.8 respectively. Whereas for a file size of 1800 kB the algorithms take 3.7, 4, 4.5 seconds respectively. As observed the time taken for decrypting increases proportionally with an increase to file size, with AES-128 taking the minimum and AES-256 taking the maximum time for file decryption

5. CONCLUSION

With the increase of data, theft attacks the security of users private data over the cloud is becoming a serious issue for cloud service providers for which, fog computing is a technique that helps in predicting and monitoring the behavior of the user and providing security to the user's data. The system was originally developed using encryption algorithm but we have also implemented it with the user could provide unprecedented levels of security in the cloud and in social network.

6. REFERENCES

[1] S. J. Stolfo, M. B. Salem and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," 2012 IEEE Symposium on Security and Privacy Workshops

[2] K. M. Reena, S. K. Yadav, N. K. Bajaj and V. Singh, "Security implementation in cloud computing using user behaviour profiling and decoy technology," 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)

[3] P.Nagendra Babu, M. Chaitanya Kumari, S. Venkat Mohan "A Literature Survey on Cloud Computing," International Journal of Engineering Trends and Technology (IJETT),

V21(6),305-312 March 2015. ISSN:2231-5381. www.ijettjournal.org. published by seventh sense research group

[4] Hamid, Hadeal & Rahman, Sk Md Mizanur & Hossain, M. Shamim & Almogren, Ahmad & Alamri, Atif. (2017). A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2757844.

[5] ASHADEEP & SACHIN MAJITHIA "ENHANCEMENT IN CLOUD DATA SECURITY USING FOG COMPUTING with Behaviour Profiling and Decoy Technology," January 2015, International Journal Articles of Engineering Research-On Reviewed International Journal

[6] S. Maqtyar Ahed , P. Namratha, C. Nagesh "PREVENTION OF MALICIOUS INSIDER IN TH CLOUD USING DECOY DOCUMENTATION", April 2017, International Journal of Engineering Research & Technology (IJERT)

[7] D. M'Raihi, M. Bellare, F. Hoornaert, and D. Naccache, "HOTP: An HMAC based one-time password algorithm, RFC 4226", Dec. 2005.

[8] Karuppiah, Marimuthu & D, Ganesh & Mehta, Harshita & Rajan, Aditya & Perumal, Boominathan. (2014). A Novel Way of Integrating Voice Recognition and one Time Passwords to Prevent Password Phishing Attacks. International Journal of Distributed and Parallel systems. 5.11-20. 10.5121/ijdps.2014.5402.

[9] Lee, Bih-Hwang & Dewi, E. & Wajdi, Muhammad. (2018). Data security in cloud computing using AES under HEROKU cloud. 1-5. 101109/WOCC.2018.8372705.

[10] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010.

[11] Wikipedia contributors, 29 May 2020, https://en.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard&oldid=959595933, Accessed on 22 December 2019.

[12] JOSH LAKE, SPECIALIST IN SECURITY, PRIVACY AND ENCRYPTION February 17, 2020 https://www.comparitech.com/blog/information-security/what-is-aes-encryption/ Accessed on February 22, 2020

[13] Difference between AES and DES Available at https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard , Accessed on February 22, 2020

[14] https://www.quora.com/How-does-the-MD5-algorithm-work

[15] https://security.stackexchange.com/questions/138363/why-is-md5-considered-a-vulnerable-algorithm

[16] Information on MD5 https://en.bitcoinwiki.org/index.php?title=MD5&action=info Accessed on March 22, 2020

[17] Cloud computing services Available on https://aws.amazon.com/types-of-cloud-computing/

[18] Types of cloud, Available onhttps://www.geeksforgeeks.org/types-of-cloud/

[19] https://md5decrypt.net/en/Sha256/