IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

Secure File Sharing: AES Encryption and Password Brute Force Detection Techniques

Prof.Jyotsna Nanajkar[1], Pratiksha Magar[2], Shreya Mote[3], Vaibhav Magar[4], Shubham Gore[5]

[1]Assistant Professor, Dept. of I.T., Zeal College Of Engineering and Research, Narhe-Pune, India

[2,3,4,5]UG Students, Dept. of I.T., Zeal College Of Engineering and Research, Narhe-Pune, India

ABSTRACT: As network data grows in volume and encryption, and high- speed networks become more widespread, it becomes increasingly challenging to detect brute-force attacks on a network level. Despite advances in research, there are still undetectable types of threats. As complete security can never be guaranteed, it is important to employ intrusion detection techniques to detect abnormal behavior quickly and minimize the impact of attackers on network performance. This study proposes an intrusion detection technique where the node (server) monitors network traffic and collects vital statistics through a monitoring software application. The administrator can then determine if an attack has taken place by examining and comparing traffic statistics.

KEYWORDS: Data breaches, Payload-based detection, Flow-based attack detection,Key request page,Data security

I. INTRODUCTION

In today's world, cloud computing has become a popular method for storing and sharing data. However, with the increasing amount of data being stored in the cloud, the risk of data breaches and unauthorized access has also increased. One of the common attacks faced by cloud data is the password brute force attack, where an attacker repeatedly tries different combinations of usernames and passwords to gain access to sensitive information.

Despite the presence of technological safeguards such as firewalls and antivirus, information and network systems are still susceptible to attacks. This is because information security involves not only technology, but also other analysis techniques. Brute-force attacks involve the use of random username and password combinations to access login credentials. In recent years, network security research has shifted towards flow-based attack detection, in addition to the established payload-based detection method. This approach examines network Flows, instead of just looking for malicious activities in packet data, due to the reduced amount of data to process and the correlation of flow data with network attacks. This study presents a detection strategy and discusses the limitations of the flow-based attack detection approach. The research aims to:

- •Document the response codes logged during login attempts
- •Evaluate the nature of the end-product with the number of login attempts
- •Provide information on the source of the attack.

Password brute force attacks are a common threat to information and network systems. They involve the use of random combinations of usernames and passwords to attempt to gain unauthorized access to a system. The increasing volume of network data and the widespread use of high-speed networks make it increasingly difficult to detect these attacks.

II. LITERATURE REVIEW

Bih-Hwang Lee. [1] explain data security in cloud computing using AES under Heroku cloud. To deploy the Heroku cloud platform for this project, there are several steps that need to be followed. The project involves creating a website that focuses on data security and uses the Advanced Encryption Standard (AES) as the encryption algorithm.. The performance evaluation shows that AES cryptography can be used as data security. In addition, calculations of data encryption delays have revealed that larger data sizes lead to increased encryption delays.

As explained by Chopade Sonali and Bade Prachi N. in their paper [2], organizations can ensure secure data storage on the cloud by using AES and ABE algorithms to encrypt their data. We can share data securely on cloud. Here, data was encrypted by sender by using public key and same can be decrypted at receiver side using private key.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

According to S. Vigneshwaran and R. Nirmalan in their article [3], even if a hacker captures data from the cloud, they would be unable to decrypt it without the private key. This ensures the security of the data stored on the cloud. Additionally, the cloud verifies the authenticity of the user without compromising their identity before storing their data. Attribute based access control has been provided in whichonlyvalid users who have matching attributes are able to decrypt the stored information in cloud. The two protocols namely attribute based encryption and attribute based signature were applied to achieve authenticatedaccess control without disclosing the identity of the user to the cloud.

M.Marwan, A. Kartit, and H. Ouahmane[6], The security framework is based on the multicloud en- vironment to store digital data at all. In order to prevent data disclosure, they practiced a segmentation approach to frag- ment the input appearance into several areas. The use of digital signature and watermarking techniques helps to ensure the integrity of outsourced clients' data, making it possible to detect any accidental changes to the data.

N.A study by A. Oussama and Z. Abdelha [7] proposed a framework that enhances the security and privacy of data by splitting it into different blocks of bits and applying a genetic algorithm to every two blocks. The output of each genetic algorithm procedure is a ciphertext along with two blocks of bits. Each ciphertext is stored on the cloud at a distinct location, making it difficult for attackers to find the exact location of the ciphertext. The use of a genetic algorithm on a small block size further increases the security of the framework, and a proficiency list is used to secure and access data.

In contrast, a framework suggested by K. Subramanian, F. L. John, and F. L. John [8] aims to store data in various clouds using 3DES and RSA encryption. However, this methodology lacks efficiency, privacy, and results in middleware overload through multiple functions.

M. Edjie, D. L. Reyes, M. Ariel Sison, and Dr. R. P. Medina [9] addressed the issue of complexity in the Mix Column conversion of AES, which was due to the dismissal of logical purposes. The modified version of AES was used to eliminate these logical tasks, resulting in a 13.6% reduction in LUTs, a 10.93% share discount, and a 1.19% reduction in interruption eating. The conservative AES was found to have a small dispersion rate at the initial entity and significant agenda sequences.

A. Arab, M. J. Rostami, and B. Ghavami,[10] The modified AES contained 10 series for encrypting, and the replacement and addition processes of the columns have been substituted by the line change and pixel standard summary. These processes not only decrease the spell complication of the algorithm but also improve the dispersal aptitude.

Author	Name Of the Paper	Year of Submission	Objective	Advantage
Bih-Hwang Lee	Data Security in Cloud Computing Using AES Under HEROKU Cloud	2018	In this paper, we discuss a secure file sharing mechanism for the cloud with the disintegration protocol and implementation of access protocol.	Data privacy and system security is enhanced.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

Chopade Sonali and Bade Prachi N	"Secure Cloud Data Using Attribute Based Encryption"	2019	data was encrypted by sender by using public key and same can be decrypted at receiver side using private key.	How organizations can store data securely on cloud by encrypting it using AES and ABE algorithms. We can share data securely on cloud.
M. Marwan, A. Kartit, and H. Ouahmane	"A framework to secure medical image storage in cloud computing environ- ment,"	2018	The security framework is based on the multicloud en- vironment to store digital data at all. In order to prevent data disclosure, they practiced a segmentation approach to frag- ment the input appearance into several areas.	The integrity of the outsourced clients' data helps to verify watermarking technique.
K. Subramanian, F. L. John, and F. L. John,	"Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system,"	2018	In this paper, the au- thors suggested a framework such that the objective is to store data in various clouds.	The given framework is found based on 3DES and RSA encryption.
M. Edjie, D. L. Reyes, M. Ariel, Sison, and Dr.R. P. Medina,	"Modified AES cipher round and key schedule,"	2019	The complexity detects were an effect of dismiss logical purposes in the MixColumn conversion of AES.	the small dispersal rate met through the conservative AES at the initial nonentity, and important agenda sequences.
A. Arab, M. J. Rostami, and B. Ghavami	"An image encryption method based on chaos system and AES algorithm,"	2019	The modified AES contained 10 series for encrypting, and the replacement and addition processes of the columns have been substituted by the line change and pixel standard summary.	The project algorithm is protected alongside the entropy occurrences.
A. Oussama and Z. Abdelha,	"A security framework for cloud data storage (CDS) based on agent,"	2019	The innovative security framework puts on a genetic algorithm on minor block size that increases the security.	The framework presented in this study is more secure, and it provides more privacy to the data. This framework splits data into different blocks of bit

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

PasswordBruteForceAttack:

A brute force attack is an attempt to guess a password or encryption key by trying every possible combination of characters until the correct one is found. To detect a brute force attack, the following measures can be taken:

1) Limit login attempts: Limiting the number of login attempts for a given user can help prevent brute force attacks.
2) Captchas: Implementing captchas on login pages can also help prevent brute force attacks.
3) IP Blocking: Blocking the IP addresses of suspected attackers can help prevent further attempts.
4) Monitoring Logs: Monitoring system logs for unusual login attempts or other suspicious activity can also help detect brute force attacks.

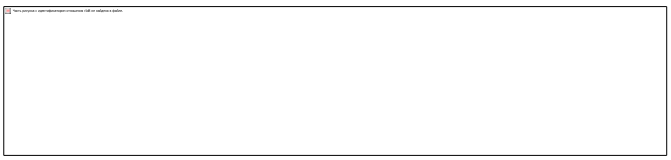

Fig 1: Brute ForceAttack

The attacker typically uses a script or program to automate the process of trying different passwords or keys, which makes the attack faster and more efficient. The script or program will try a large number of possible combinations until the correct password or key is found.

To protect against brute force attacks, it is important to use strong passwords or encryption keys that are long and complex. Additionally, systems can implement measures such as limiting the number of login attempts or introducing a delay between login attempts to make brute force attacks more difficult and time- consuming. It is also important to monitor system logs for unusual login activity and take appropriate actions when necessary.

ProtectingDatawithAESEncryptionAlgorithm:

AES (Advanced Encryption Standard) is a symmetric encryption algorithm used to protect sensitive data. It uses a symmetric key, meaning the same key is used to encrypt and decrypt the data. AES is considered a secure encryption algorithm because it uses a block cipher with a fixed block size of 128 bits.

To encrypt data using AES, the following steps are followed:

1) Choose a secret key: The secret key is used to encrypt and decrypt the data. It should be kept secret and not shared with anyone.
2) Choose a block cipher mode: There are several block cipher modes, such as CBC (Cipher Block Chaining) and ECB (Electronic Codebook), that determine how the data is encrypted.
3) Apply the encryption algorithm: The encryption algorithm is applied to the plaintext data using the secret key and block cipher mode.
4) Store the encrypted data: The encrypted data can be stored in a database or sent over a network.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

AES, also known as the Advanced Encryption Standard, is a type of encryption algorithm that utilizes symmetric key encryption to safeguard sensitive information.It is widely used in various applications, such as online banking, file encryption, and secure communication.

The AES encryption algorithm operates on data in fixed-size blocks, making it a block cipher. The block size used in AES encryption is determined by the key size chosen, with options for 128-bit, 192-bit, and 256-bit keys.The larger the key size, the more secure the encryption, but also the slower the encryption process.

AES encryption involves several rounds of substitution, permutation, and linear transformations. During the encryption process, plaintext is divided into blocks, and each block is encrypted separately. The encryption key i s used to determine the transformations performed on each block.

AES decryption is the reverse process of encryption, where the encrypted data is transformed back into plaintext using the same key.

In summary, AES is a highly secure encryption algorithm that provides confidentiality and integrity to data. It is widely used in various applications to protect sensitive data from unauthorized access.

III. PROJECT OVERVIEW

The proposed system enables organizations to store data securely on the cloud using AES encryption. Data sharing on the cloud is also secure as it is encrypted by the sender using a public key, which can only be decrypted by the receiver using a private key. This way, even if a hacker intercepts the data, they cannot access it without the private key, ensuring the data remains secure on the cloud.

The system collects information on the login attempts, including the response codes and the nature of the end-product. The data is then analyzed to determine the initiator of the attack. The AES encryption algorithm is used to encrypt data before it is stored on the cloud, ensuring its security.

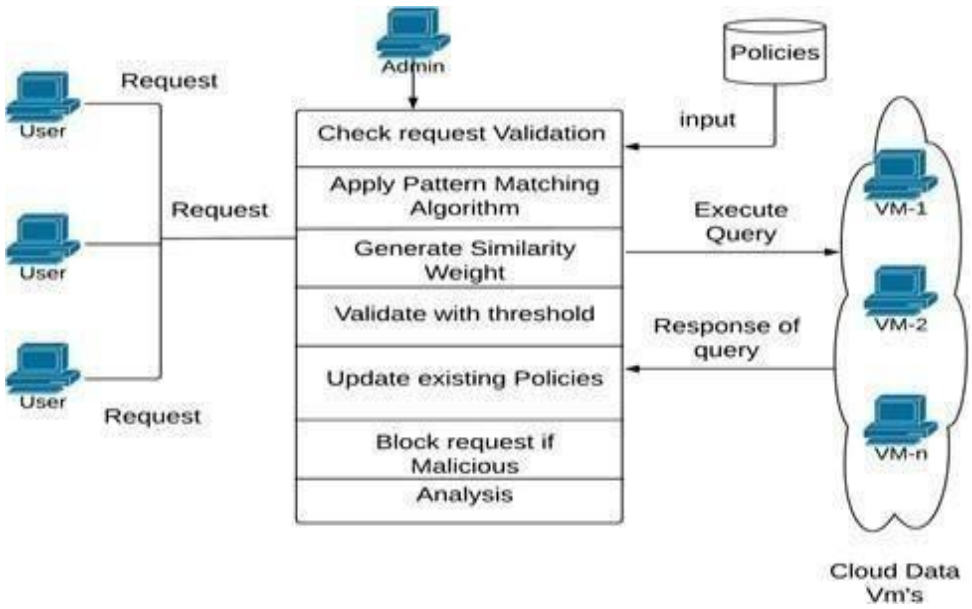

Fig 2: System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

IV. PROPOSED ALGORITHM

The proposed model consists of two main components: the brute force attack detection system and the data encryption system. The brute force attack detection system uses AES encryption to encrypt data before it is stored on the cloud, ensuring its security.

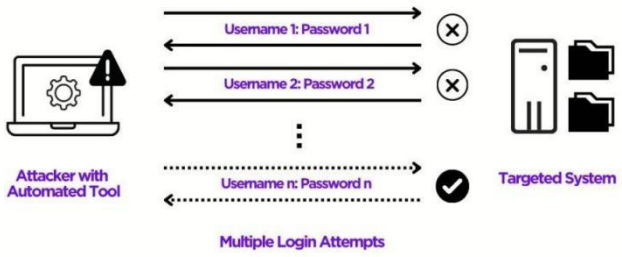

Fig 3: Proposed Implementation

A.System Implementation:

The proposed system aims to secure both text and PDF files. The Advanced Encryption Standard (AES) algorithm is employed for encryption and decryption of the files. Upon uploading of the files to the cloud storage, the files are encrypted using AES. When the user downloads the files, the decryption process using the inverse of the AES algorithm takes place to make the file accessible.

B.Password brute-force attack detection:

The proposed system is designed to enhance the security of web applications by protecting against password brute force attacks. The system requires users to create an account and uses default credentials for the admin account. The system will notify both the admin and the user after a certain number of incorrect password attempts. This allows the admin to detect and block the IP address of the attacker, providing a robust and effective defense against brute force attacks. The system is aimed at improving the security of web applications and providing a safer user experience.

C.Admin Panel:

In this system, the Admin has complete control over the data stored on the cloud. They have the ability to edit, modify, create, share and restrict access to the data. In traditional systems, the cost of setting up servers and maintaining them is high for a business owner. However, in this system, the Admin can access and manage the data stored by the Cloud Service Provider, eliminating the need for expensive server setup and maintenance.

The file upload section allows users to upload files in either .txt or .pdf format. Once uploaded, the file is encrypted using the AES algorithm in the cloud/virtual machine. The encryption section of this module uses the AES algorithm to generate encryption for text files. When the Admin uploads the text files to the Cloud Storage, they are encrypted, and only the inverse of the AES algorithm can be used to decrypt the file when the user downloads it, providing increased security.

D.User Panel:

In this system, users can access data stored on the cloud by the Admin at any time. The Admin will share the requested data stored on the cloud database with the user. The users can search for their desired files in the cloud storage that have been uploaded by the Admin. These files are in encrypted format, so the user must request the Admin for the key to decrypt the file and download it. The key request can be sent through the key request page of the user panel. With the key provided by the Admin, the user can then decrypt the file and download it for their use.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103059|

V. CONCLUSION AND FUTURE WORK

In this project, we proposed a system that combines the detection of Password Brute force attacks and the protection of cloud data. The system employs AES encryption algorithm to encrypt the data before it is stored on the cloud. The user requests a key from the Admin to access the encrypted data, and the Admin has the authority to grant or deny the request.

The system also employs data mining techniques to detect Password Brute force attacks. Raw data from the Internet and real-time malicious activities were collected and processed to create a background knowledge database. The testing phase involved the simultaneous collection of real- time and real data, which was then processed and used to train the system using a similarity algorithm.

Based on the experiment's findings, the proposed system has demonstrated a high level of accuracy and precision in detecting both benign activities and Password Brute Force attacks. The combination of AES encryption and Password Brute force detection ensures the security of cloud data and reduces the risk of unauthorized access.

REFERENCES

[1] "Data Security in Cloud Computing Using AES Under HEROKU Cloud" was published by Bih-Hwang Lee in2018 and presented at IEEE.

[2] "Secure Cloud Data Using Attribute Based Encryption," was authored by Chopade Sonali and Bade Prachi.N and also published in IEEE in 2019.

[3]"Attribute based Encryption on Secret Verification in Cloud" and authored by S. Vigneshwaran and R. Nirmalan Rin 2015.

[4] "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud," was published in 2019 and authored by Yujiao Song and Hao Wang.

[5] Authored by Avinash N and Divya C, is titled "An Attribute Based Encryption for Accessing Data on Cloud" and was published in IEEE.

[6] M. Marwan, A. Kartit, and H. Ouahmane, “A framework to securemedical image storage in cloud computing environ-ment,” *Journal ofElectronicCommerceinOrganizations*,vol.16,no.1,pp.1–16,2018.

[7] Authored by A. Oussama and Z. Abdelha, is titled "A security framework for cloud data storage (CDS) based on agent" and was published in the journal Applied Computational Intelligence and Mathematical Methods by Springer in 2019.

[8] "Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid cryptography system," was published in the International Journal of Advanced and Applied Sciences in 2018. It was co-authored by K. Subramanian and F.L. John.

[9] Authored by M. Edjie, D.L. Reyes, M.A. Sison, and Dr. R.P. Medina, is titled "Modified AES cipher round and key schedule" and was published in the Indonesian Journal of Electrical Engineering and Informatics (IJEEI) in March 2019.

[10] "An Image Encryption Method Based on Chaos System and AES Algorithm," was authored by A. Arab, M.J. Rostami, and B. Ghavami and was published in the Be Journal of Supercomputing in 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details