

# Detecting Password Brute Force Attack and Protecting the Cloud Data with AES Encryption Algorithm

Prof. Jyotsna Nanajkar<sup>1</sup>, Pratiksha Magar<sup>2</sup>, Shreya Mote<sup>3</sup>, Shubham Gore<sup>4</sup>, Vaibhav Magar<sup>5</sup>

<sup>1</sup>Assistant Professor, Dept. of I.T., Zeal College of Engineering and Research, Narhe, Pune, India

<sup>2,3,4,5</sup>UG Students, Dept. of I.T., Zeal College of Engineering and Research, Narhe, Pune, India

**Abstract:** *Brute-force attacks are common, and as network throughput and encryption grow, and high-speed networks become ubiquitous, brute-force attacks at the network stage will become increasingly difficult to detect. Despite progress in research in this area, there are still many undiscovered threats. Because no security solution can guarantee that attackers will not succeed in time, access detection technology must be used to detect divergent behavior early and reduce the impact of intruders on network operations. This work presents a method to identify nodes (servers) monitoring traffic in the network and collect important statistics using a monitoring software application. By analyzing and comparing traffic statistics, administrators will be able to determine if an attack has occurred.*

**Keywords:** brute force, attack, security, cloud

## I. INTRODUCTION

Even with the best protections like firewalls and antivirus soft ware, data and network systems are vulnerable. This is because data security includes not only study but also other research that ensures correct identification. Brute force attacks use random username and password combinations to authenticate login credentials. In recent years, research on network security has begun to focus on counter-attacks in addition to information-based payment methods. It not only looks for malicious activity in actual packet data, but also inspects traffic on the network.

This is not surprising because there is less data to contend with and attacks are obvious on streaming data such as networkloads. We present the search strategy and discuss the shortcomings of the escape detection method. The research is given to complete the following points:

1. Encrypt data using the AES algorithm.
2. The nature of the final product and the number of trial entries
3. Attack initiator information.

In order to ensure data security on cloud-based servers with data storage, the main problem arises from preventing access by unauthorized persons. Information security must strike a balance between security and usability. In order to ensure that user information is very secure in case users lose access to the data after accessing it in the cloud, AES encryption technology will protect the data from being stolen or lost.

## II. PROJECT OVERVIEW

In this offering, organizations can access data using the AES algorithm and securely store data in the cloud. We can share data securely in the cloud. Here the data is encrypted by the sender using the public key and can be decrypted by the receiver using the private key. So even if the data is compromised by the hacker and cannot decrypt it until they get the private key, the data is safe in the cloud.

Website applications are widely used in many enterprises, while they are providing convenience, the web application brings a lot of the security risks. Password is the first line of defense in the web application, the low level password problem has always been a short board in web application security protection system.

In this system user should create an account, admin account credentials are default. when the attacker tries to bruteforce the password using any method. The admin and user both will be notified after certain number of

wrong passwords attempts .After detecting the attack admin will have the rights to block the IP address of the attacker .

### III. LITERATURE SURVEY

Bih-Hwang Lee. [1] Explains data security in cloud computing using AES under Heroku cloud.The process of deploying Heroku as a cloud platform consists of several steps. This project uses a web-based application for data security. On the website, we use theAdvanced Encryption Standard as the data security algorithm. Performance tests show that AES cryptography can be used.a security. In addition, the latency calculation for data encryption shows that data size increases the data latency of encrypted data.

Chopade Sonali and Bade Prachi N. [2] describe how organizations can securely store data in the cloud by encrypting it using AES and ABE algorithms. We can share data securely in the cloud. Here the data is encrypted by the sender using the public key and can be decrypted by the receiver using the private key. So even if the data is compromised by the hacker and cannot decrypt it until they get the private key, the data is safe in the cloud.

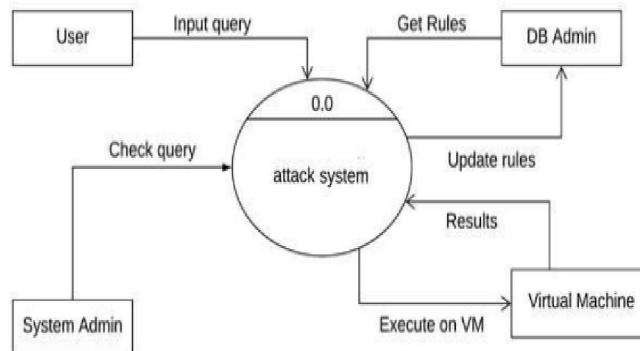
S.s.Vigneshwaran and R. Nirmalan. R.[3] explains that the cloud authenticates the user without recognizing the user before storing the data. Access-based behavior control is provided and only valid users with relevant attributes can determine data stored in the cloud. Use two methods, attribute-based encryption and attribute-based signing, to enforce effective access control without revealing the user's identity to the cloud.

### IV. SOFTWARE DESIGN

#### 3.1 Data flow diagram

Data Flow Chart (DFD) is a graphical representation of the flow of information through information systems. p.w.m. A Flow Chart (DFD) is used as the first step in creating a system overview with out having to enter the details. The lighting element is the top level or LEVEL 0 data flow graph.

It has a transaction node that summarizes the functionality of the entire system in relation to other organizations. Data Flow Chart (DFD) layer. Draw the diagram first, then draw the data flow or process at different levels.



**Fig -1: Dataflow Diagram-level 0**

#### 3.2 System Implementations

The proposed system is designed to maintain security of not only (.txt ) files but also (.pdf ) files . Given proposed system uses Advances Encryption Standard algorithm to perform encryption and decryption. When Admin uploads the pdf or text files in Cloud Storage, the file is encrypted. Inverse of the AES algorithms are used to decrypt the file when the user downloads it from Cloud Storage .

### V. FUTURE SCOPE

Brute-force attacks are a common way for attackers to try to gain access to protected data. In a brute-force attack, the attacker tries every possible combination of characters until they find the correct password. This can be a very time-consuming process, but it is possible if the attacker has enough computing power.

There are a number of ways to detect brute-force attacks. One way is to look for a sudden increase in the number of failed login attempts. Another way is to look for patterns in the failed login attempts. For example, if the attacker is trying every possible combination of letters and numbers, then the failed login attempts will likely be in alphabetical order.

Once a brute-force attack has been detected, there are a number of things that can be done to protect the data. One way is to increase the complexity of the passwords. Another way is to use two-factor authentication. Two-factor authentication requires the user to enter a code from their phone in addition to their password. This makes it much more difficult for an attacker to gain access to the account, even if they know the password.

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that is widely used to protect data. AES is a very strong encryption algorithm, and it is very difficult to break. However, it is important to use a strong key when encrypting data with AES. A weak key can make it easier for an attacker to break the encryption.

The future scope of detecting password brute force attacks and protecting data with AES encryption algorithm is very promising. As technology continues to evolve, so too will the methods that attackers use to try to gain access to protected data. By using strong passwords and two-factor authentication, organizations can make it much more difficult for attackers to succeed.

In addition to the methods mentioned above, there are a number of other ways to protect data from brute-force attacks. These include:

Using a password manager to generate and store strong passwords

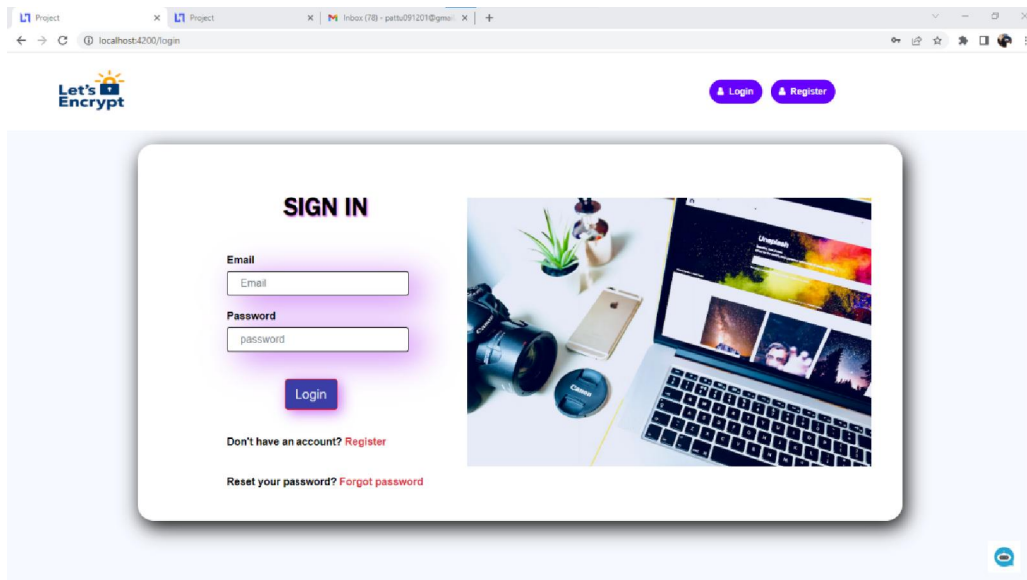
Using a firewall to block unauthorized access to your network

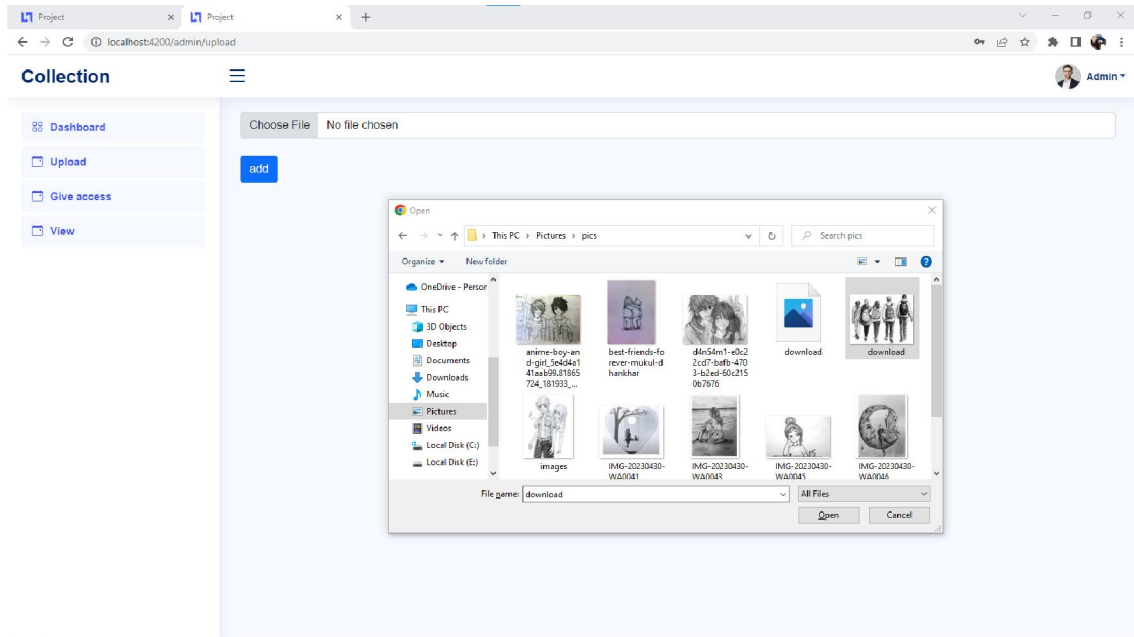
Keeping your software up to date with the latest security patches

Educating your employees about security best practices

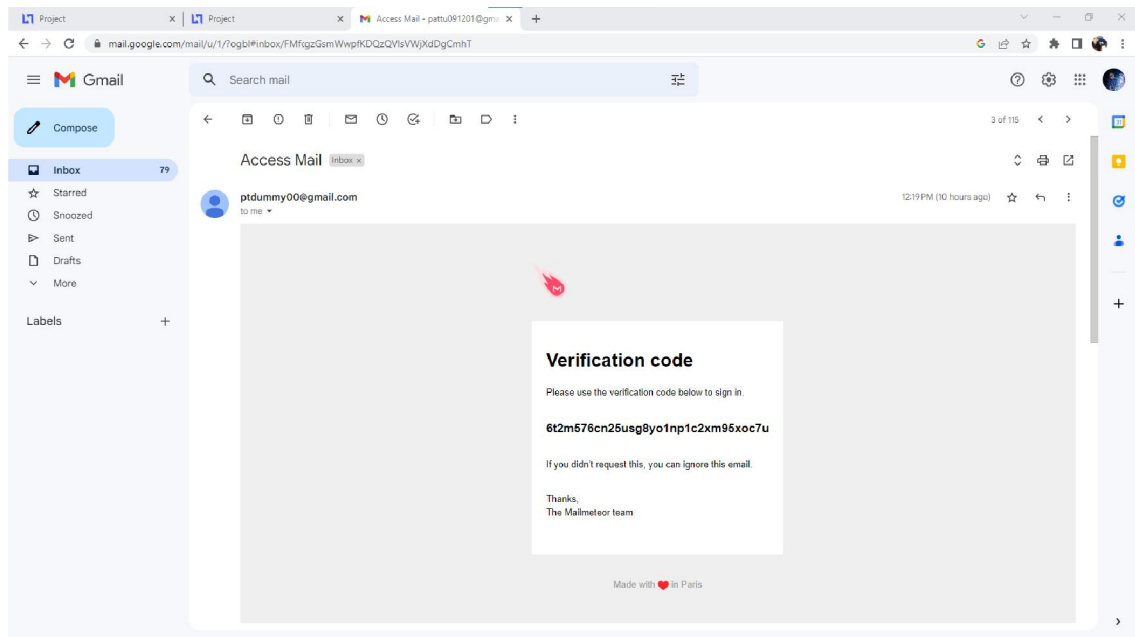
By taking these steps, you can help to protect your data from brute-force attacks and other security threats.

## VI. RESULTS

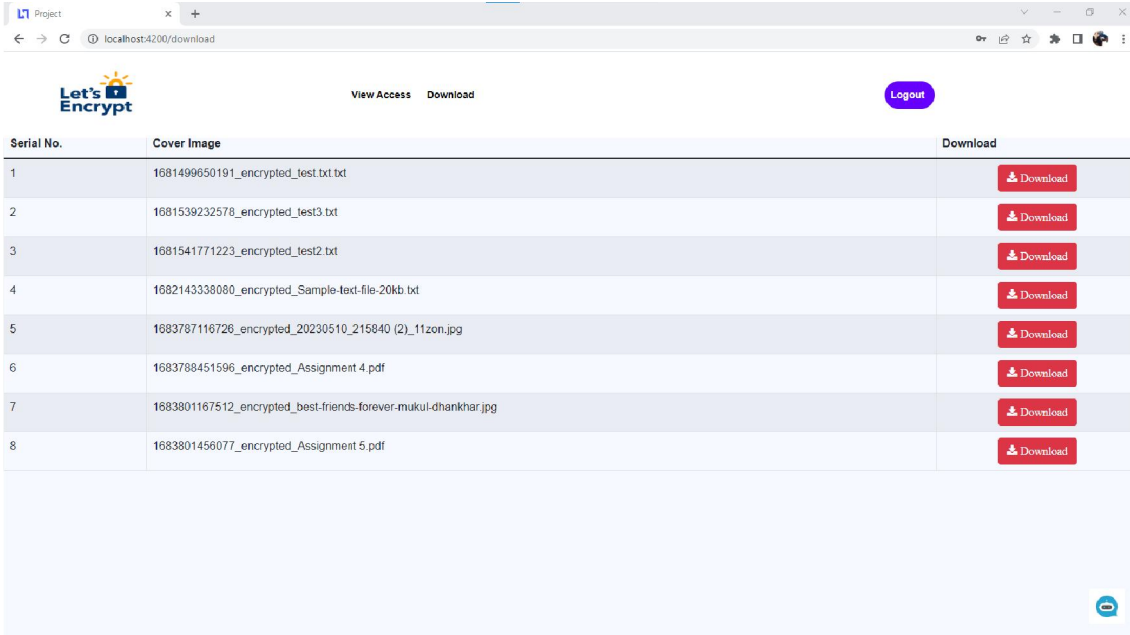




**Fig -3: Uploading data**



**Fig -4: Key Generation**



Serial No.	Cover Image	Download
1	1681499650191_encrypted_test.txt	<a href="#">Download</a>
2	1681539232576_encrypted_test3.txt	<a href="#">Download</a>
3	1681541771223_encrypted_test2.txt	<a href="#">Download</a>
4	1682143338080_encrypted_Sample-text-file-20kb.txt	<a href="#">Download</a>
5	1683787116726_encrypted_20230510_215840 (2)_11zon.jpg	<a href="#">Download</a>
6	1683788451596_encrypted_Assignment 4.pdf	<a href="#">Download</a>
7	1683801167512_encrypted_best-friends-forever-mukul-dhankhar.jpg	<a href="#">Download</a>
8	1683801456077_encrypted_Assignment 5.pdf	<a href="#">Download</a>

**Fig -5: Data Download by users**

## VII. CONCLUSION

Detecting password brute force attacks and protecting data with AES encryption algorithm are essential components of a comprehensive security strategy. By implementing measures to detect and mitigate brute force attacks, organizations can reduce the risk of unauthorized access and data breaches. Additionally, AES encryption provides a strong layer of protection for data at rest and in transit, ensuring confidentiality and integrity.

The use of techniques such as account lockouts, CAPTCHA or reCAPTCHA challenges, rate limiting, intrusion detection systems, and user behavior analytics can significantly enhance the detection and prevention of password brute force attacks. These measures create barriers that make it difficult for attackers to gain unauthorized access through repeated login attempts.

On the other hand, AES encryption algorithm provides a robust method for protecting sensitive data stored on cloud servers. It ensures that even if an unauthorized party gains access to the data, they would be unable to decrypt and make sense of it without the encryption key. Additionally, encrypting data during transmission using protocols like TLS prevents interception and eavesdropping.

In conclusion, combining effective techniques to detect password brute force attacks with the implementation of strong encryption algorithms like AES provides a solid foundation for safeguarding sensitive data. However, it is important to remain vigilant, keep abreast of the latest advancements in cybersecurity, and continuously evaluate and enhance security measures to stay one step ahead of potential threats.

## REFERENCES

- [1]. Chauhan, A., & Gupta, B. B. (2019). A Secure Key Management Scheme using AES Algorithm for Cloud Computing. In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT) (pp. 165-170). IEEE.
- [2]. Das, S., Kar, S., & Bhattacharya, B. B. (2019). A Machine Learning Approach for Detecting Brute-Force Attacks in Cloud Computing Environment. In Proceedings of the 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 602-607). IEEE.
- [3]. Garnaeva, M., & Pavlov, A. (2019). Detecting Brute-Force Attacks in Web Applications with Machine Learning Algorithms. In Proceedings of the 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-6). IEEE.

- [4]. Singh, S., & Rani, R. (2019). Detection of Brute-Force Attacks on Remote Authentication System in Cloud Computing Environment. In Proceedings of the 2nd International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 453-457). Springer.
- [5]. Zhu, C., Xu, M., & Chen, X. (2019). Detecting Brute Force Attacks Against Remote Authentication Services Based on Convolutional Neural Networks. In Proceedings of the 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 185-189). IEEE.
- [6]. Arul Kumar, R., Anuradha, S., & Saravanakumar, R. (2020). A Secure Approach for Data Storage and Access Control in Cloud Computing using AES Encryption and Attribute-based Access Control. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
- [7]. Maurya, P., & Bhatt, A. (2020). A Secure Data Storage System in Cloud Computing Using AES Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering, 10(9), 194-201.
- [8]. Rahman, M. S., & Biswas, G. P. (2020). Detection and Prevention of Brute Force Attack in Cloud Environment. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.
- [9]. Sharma, A., & Bhatnagar, S. (2020). An Enhanced AES Algorithm for Cloud Data Security. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
- [10]. Zhang, Q., Guo, C., Li, Y., & Jin, H. (2020). A Distributed Brute-Force Attack Detection System in Cloud Computing. In Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-3). IEEE.
- [11]. Jin, D., Li, J., Zhang, J., & Wang, H. (2019). Detecting Brute-Force Attacks Against Remote Access Services in Cloud Computing Environment. IEEE Access, 7, 57755-57764.
- [12]. Liu, Z., Qiu, J., Qiu, S., & Shi, W. (2020). Secure Data Storage and Access Control Scheme in Cloud Computing Based on AES and HMAC. International Journal of Grid and Distributed Computing, 13(2), 115-126.
- [13]. Raza, A., Xu, X., & Xie, J. (2020). Brute-Force Attack Detection for Internet of Things (IoT) Based on Machine Learning. In Proceedings of the 2020 IEEE International Conference on Internet of Things and Intelligence System (IoT&IS) (pp. 312-316). IEEE.
- [14]. Rehman, M. H., Saeed, U., Saleem, M. S., Mahmood, T., Rehman, S. U., & Maqsood, M. (2020). Intelligent Intrusion Detection System Using Machine Learning Techniques for Brute Force Attacks. IEEE Access, 8, 169098-169108