GE-International Journal of Engineering Research
ISSN(O): 2321-1717, ISSN(P): 2394-420X
Vol. 8, Issue 05, May 2020 Impact Factor: 5.779

www.aarf.asia,**Email** : editor@aarf.asia, editoraarf@gmail.com

ENHANCING SECURITY TO OVERCOME EDoS ATTACK IN CLOUD

Ms. K. Manasa, M.Tech. Student,
Department of Computer Science &Engineering,
Sreenidhi Institute of Science & Technology, Hyderabad.

Mrs. Doddi Srilatha, Assistant Professor,
Department of Computer Science &Engineering,
Sreenidhi Institute of Science & Technology, Hyderabad.

Dr.Prasanta Kumar Sahoo, Professor,
Department of Computer Science &Engineering,
Sreenidhi Institute of Science & Technology, Hyderabad.

ABSTRACT

Cloud computing model provides on demand services in computer era. But we cannot trust fully on cloud providers, lots of providers sell users data to large companies for their own profit. Because there is no communication between cloud provider and user mainly with public clouds. Public clouds are storing users data in plain text form which is vulnerable to read users data easily in the clouds. For sharing information with users ciphertext-policy attribute-based encryption (CP-ABE) is used to secure the data in the clouds. Attackers can use brute force attack against CP-ABE encryption which can easily break security levels. With CP-ABE is not good enough to decrypt and encrypt data which is stored in the cloud. Attackers can easily download data from cloud and even can launch Economic Denial of Sustainability (EDoS) attack. CP-ABE consume the high amount of cloud resource. Resource-exhaustion attack and resource consumption accountability are possible which can lead to consume more resources and waste of money. Cloud providers cannot give full access to users to control their data or files, attackers still uses their own techniques to bypass security levels to get access to users data files. In the proposed system, AES 256 bit encryption technique is used to achieve high security for users data and minimum resources to secure the users data in the cloud which can save user data and money. It does not required any type of certificates like SSL to secure the data. The OSINT(open source intelligence) collects data from the internet sources which we cannot find in normal browsers. It checks weather the IP is malicious or not, if IP is malicious then it sends alert message to admin. With this we can easily stop EDoS attacks from the attackers.

KEYWORDS: **Public cloud storage, AES, Anti EDoS model, OSINT.**

1. Introduction:

Cloud computing is the one of the most used platform by organizations and individuals. Cloud computing is very popular due to its flexibility and easy to access services. In cloud, users can store their data and that can be accessed over the Internet. Most of the people use public clouds because services are available at free of cost. Private clouds are costly and used for storing business information of single organization. Anyhow public cloudcannot provide high security to users data. Generally cloud providers gives access to cloud services based on "pay-more only as costs arise" model, with this they can suddenly raise cost of services to users. Companies or cloud providers give assurance to people to use their applications with easy and simple manner without any confusion to users, supporting to users with customer support services with improved security features. Whenever cloud service provider give update to users for their application or data then users need not to worry about their data because cloud service providers always maintains backup servers for data security. Cloud providers always create workspace through Virtual Private Networks(VPNs). Within this workspace users can do their operations without any enlarge in their works. Users can store any kind of data in the cloud server or storage devices.

Companies always try to provide services with low cost by give their services and space in their storage servers. User can modify frameworks according to users wish to work in easy way without any interruption in the work. If user is providing any services to another users then framework should be more reliable to work conveniently to users. Dispersed processing loosened up this breaking point to cover all servers similarly as the framework system. The target of disseminated figuring is to allow customers to take benefit by these advances, without the necessity for significant data about or capacity with each and every one of them. The cloud intends to lessen costs and empowers the customers to focus on their middle business instead of being obstructed by IT hindrances. Encryption doesn't itself hinder block anyway denies the reasonable substance to an inevitable interceptor. To do encryption, computer requires huge resources to complex algorithms, sometimes encryptions can be done without any key also but it will be very complex to get original content. Encryptions always does converting readable message to unreadable data format which will makes secure the data from the attacker. Attacker always tries to watch data in the network itself only without getting cough by the users or service providers.Encryptions and cryptography have been used

by many organizations and mainly secret organizations and militaries and governments to secure their communications. It is at present normally used in making sure about information inside various sorts of non military work force structures. For example, the Computer Security Institute reported that in 2007, 71% of organizations read utilized encryption for a segment of their data in movement, and 53% utilized encryption for a bit of their data away. Encryption is a significant instrument yet isn't adequate alone to guarantee the security or protection of touchy data all through its lifetime. Most utilizations of encryption ensure data just very still or in travel, leaving delicate information in clear text and possibly defenseless against inappropriate divulgence during preparing, for example, by a cloud administration for instance. Homomorphic encryption and secure multi-party calculation are developing strategies to register on scrambled information; these methods are general and Turing finish yet acquire high computational as well as correspondence costs. Cryptography concept is every advanced technique to encryption of data files or communication while transmission of data from sender to receiver. The originator of an encoded message shares the deciphering system just with expected beneficiaries to block access from enemies. The cryptography composing every now and again uses the names Alice ("A") for the sender, Bob ("B") for the proposed recipient, and Eve ("spy") for the foe. Open-source insight (OSINT) is information gathered from freely accessible sources to be utilized in a knowledge setting. In the knowledge network, the expression "open" alludes to clear, freely accessible sources (instead of incognito or surreptitious sources). It isn't identified with open source programming or aggregate insight.The catchphrase behind OSINT idea is data, and above all, data that can be gotten for nothing. It doesn't make a difference on the off chance that it is situated inside papers, websites, pages, tweets, online life cards, pictures, digital broadcasts, or recordings as long as it is sans open and legal.With the correct data in your grasp, you can get an extraordinary bit of leeway over your opposition, or accelerate any organization or individual examination you are accountable for.

1.1 Existing System:

Whenever attacker launches EDoS on client server or cloud storage then consuming of resources getting high in the cloud or client server, which is lose to user because without using resources users have to pay, whenever this attack occurred on client server or cloud storage. In the existing system it has only 64 bit encryption which has very low level security. Attackers can easily break this encryption with advanced decryption tools. Existing works use CP-ABE used for encryption, which makes much more vulnerable to user data files. Public clouds are not able to provide much security to users, with this loophole attackers used attacks on cloud sever which makes economically lose to users, it leads to EDOS attack. Depends on attack strength user will get affected.

1.2 Proposed System:

In this paper, Anti EDOS Model is proposed with the help of open source intelligence to find out the malicious user. This can helps to find malicious user based on IP address. Whatever attacker uses to attack on cloud server the proposed system will finds it out and alert the admin with email alert system. To secure users files, used AES256 bit key size encryption which makes very hard time break it. With the proposed system users will get lots of benefits because they are getting multiple security levels which makes impossible to break the security levels of users. If incase attacker uses the latest IP to attack for EDoS then application checks for requests count, normally user can send requests up to 10-15 , so it waits up to 20 or 30 , later it will gives alert message to owner and keeps the attacker in black list.

The advantages of proposed system are: encryption levels are high, data steeling is not possible, and resources are consumed less. The architecture of proposed system is shown in Figure 1 and is explained in Section 2.

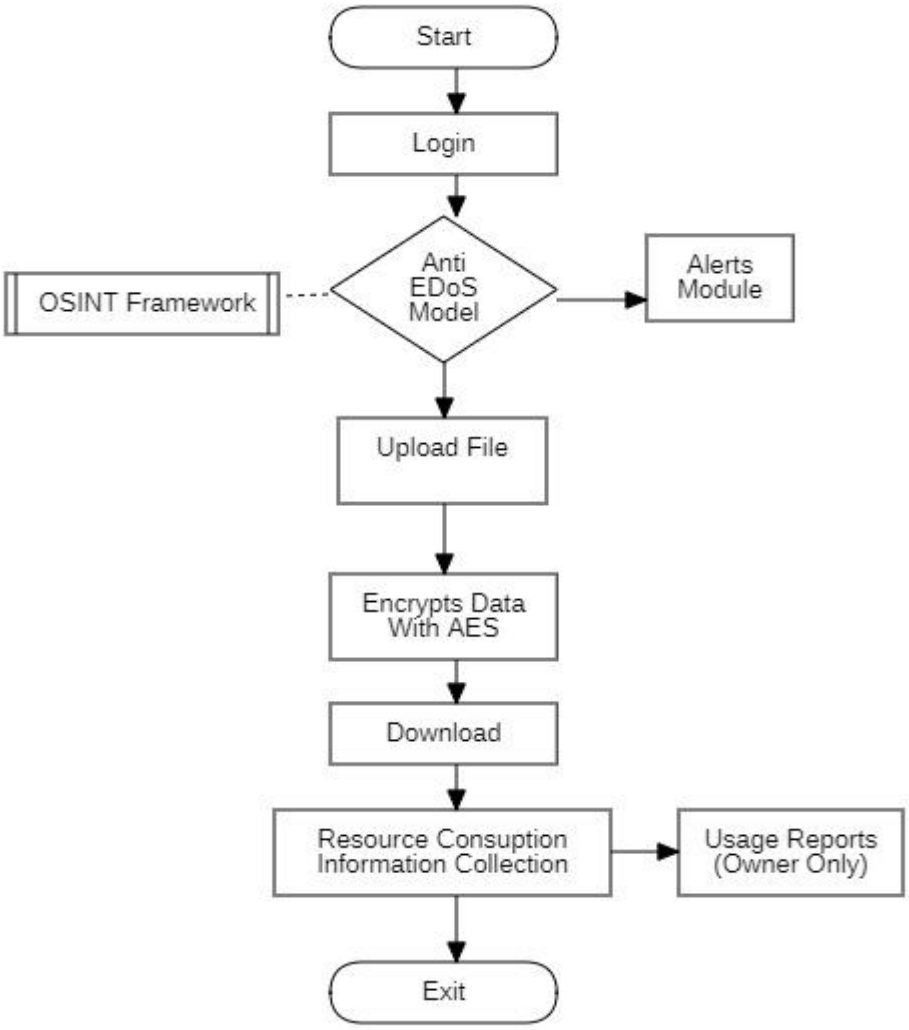

Figure 1. The Architecture of Proposed System

The organization of paper is as follows: Related works are discussed in section 2 and section 3 discussed about implementation and results and section 4 is the conclusion.

Related Work:

To keep sensitive customer data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. It is overcome by Key Policy Attribute-Based Encryption (KP-ABE)[1]. Encryption can be done by user defined key. When in doubt apply cryptographic systems by revealing data unscrambling keys just to affirmed customers. In any case, these are offering keys to everyone whoever demands that the key cloud with least information about customers. The issue of simultaneously achieving fine-grainedness, flexibility, and data confidentiality of access control as a general rule in spite of everything remains unsure. This work is acceptable under standard cryptographic conditions or models.

Attribute based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Used Ciphertext-Policy Attribute-Based Encryption[2]. Documents can be changed into ciphertext in easy way. Performs AND and OR operations to change of documents. The drawback of this example is that it is continuously getting challenge to cloud service providers to give assurance of security issues; when data is taken care of at a couple of zones, the chances that one of them has been undermined increases definitely.

Generally attackers uses different kinds of techniques to steal user passwords with knowing to user and without getting by the user. Basically they user phishing pages, key loggers and trojens or virus. But most dangerous method is man in the middle attack, with this attacker can watch everything users activities without knowing to users. Using of weak passwords and same passwords for many other applications. Using credentials in untrusted computers. Overcome by user authentication protocol named oPass.[3]. Users' traffic will pass from oPass Protocols, which makes different credentials to every site but not to user. People are more skilled in recollecting graphical passwords than content passwords, numerous graphical secret phrase plans were intended to address human's secret phrase review issue. Late days Facebook and Google confronted same issue. These organizations as well as part numerous organizations are confronting same issue. Sparing passwords in plain content is a major danger to clients since aggressors can take or can see their passwords and can sell them for their benefits. A few examines center around three-factor verification as opposed to secret phrase based validation to give progressively solid client confirmation. Three-factor verification relies upon what you know (e.g., secret key), what you have (e.g., token), and what your identity is (e.g., biometric). 1.5% of Yahoo clients overlook their passwords consistently. Assailants can introduce malwares and set up a secondary passage to gather a client's delicate information(e.g.passwords).

The paper [4] shows as increasingly touchy information is shared and put away by outsider locales on the Internet, there will be a need to encode information put away at these destinations. One disadvantage of scrambling information is that it tends to be specifically shared just at a coarse-grained level (i.e., giving another gathering your private key). The authors build up another cryptosystem for fine-grained sharing of encoded information that is namely Key-Policy Attribute-Based Encryption (KPABE). The paper [5] presents another sort of encryption techniques called Fuzzy Identity-Based Encryption (Fuzzy IBE). The

Fuzzy IBE takes into account a private key for a character, ω, to unscramble a figure content scrambled with a personality, ω_, if and just if the characters ω and ω_ are near one another as estimated by the "set cover" separate measurement.

In the proposed system, first user or owner logins into application. Then the system checks for malicious IP's with the help of OSINT Framework. Here, Open source intelligence is the data collected from publicly available sources to be used in an intelligence context. It helps to find out blacklisted IP's. Next, the system applies Anti EDoS model to check any attack or malicious IP. If found it gives alert to owner and finally, the system applies encryption with AES 256 algorithm on user files while uploading to the server. The user or owner downloads the files and server collects usage information. The owner utilizes the report function to get the overall usage information.

2. Implementation and Results:

The proposed system uses Advanced Encryption Standard (AES) technique for encryption. This technique works as follows.

The AES encryption algorithm takes 16-bit block of plain text as input and gives a 16-bit block of cipher text as output. Usually key size is 128 bits, or192 bits, or 256 bits. Here number of rounds depends upon the key size:

For 128 bits, the number of rounds are 10, 192 bits, the numbers of rounds are 12 and 256 bits, the number of rounds are 14.

In this algorithm plain text is represented in the form of matrix which is known as state.For all the rounds except last round we need to apply four transformations. The four transformations are:

1. **Substitute Byte:** A Byte is replaced by another byte. Every byte has 8 bits in this first four represents row numbers and second four represents column numbers.
2. **Shift Rows:** Here rows are shifted based on row number
   Row 0-No change.
   Row 1-One left circular shifts.
   Row 2-Two left circular shifts.
   Row 3-Three left circular shifts.

3. **Add Mix Columns:** We need to separate each column in a matrix and multiply it with constant or fixed matrix. Fixed matrix contains three values they are 1, 2, 3.

4. **Add Round Key:** from key expansion we are getting a key is added to plain text which comes from a previous state. To generate new key perform XOR operation for plain text and newly generated key.

The proposed system achieved good results when comparing with existing systems. It provides better security. The system gives hard time to attackers to break encryption.

The results of the proposed system are shown in Table 1. We consider the accuracy, precision, true positive, false positive metrics for the system's performance evaluation.

Accuracy refers to the correctly predicting the class labels. It is calculated by the ratio of correctly classified instances to the total number of instances.

True Positive is an outcome where the model correctly predicts the positive class. It is the accurate prediction.

False Positive is an outcome where the model correctly predicts the negative class. It mainly predicts the incorrectly classified instances.

Therefore, for the given location and encryption the system achieves an accuracy of 95%.

The performance of proposed system is better than existing techniques such as Ciphertext-Policy Attribute-based Encryption (CP-ABE), and Imprint based IDS(Intrusion Detection System).

	Anti EDoS	**(CP-ABE)**	**IDS**
Accuracy	**97**	**60**	**70**
Precision	**0.831**	**0.980**	**0.831**
True Positive	**0.830**	**0.98**	**0.740**
False Positive	**0.202**	**0.102**	**0.12**

Table 1: Results of proposed system and comparison with existing systems.

4. Conclusion:

Anti-EDoS model is successfully developed to prevent from the EDoS attacks. Security levels in the encryption have been increased. It upgraded to 256 bit key size encryption which makes more secure to users data file and severs. The proposed works with open source intelligence. So the proposed system is available at free of cost and it consumes less amount of resources.

References:

[1]. Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

[2]. John Bethencourt, amitsahai, brent waters,"Ciphertext-Policy Attribute-Based Encryption", Supported by NSF CNS-0524252 and the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.

[3]. Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin," oPass: A User Authentication Protocol Resistant to PasswordStealingandPasswordReuseAttacks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.7, NO.2, APRIL 2012.

[4] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98). Acm.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–Eurocrypt 2005. Springer, 2005, pp.457–473