Implementation of DDoS Attack Preemption and Improved Data Integrity in Cloud

Ashwini Khadke
Department of Computer
Science and Engineering
G.H Raisoni College of
Engineering Nagpur, India

Mangala Madankar
Department of Computer
Science and Engineering
G.H Raisoni College of
Engineering Nagpur, India

ABSTRACT

Nowadays mobile phone is a basic need for everyone. Mobile Cloud Computing is a very convenient & on- demand network access of the shared resources like services, network, applications, Servers & cloud data storages. DDoS attack can be possible on mobile cloud as well as data integrity can also be possible on data stored on mobile cloud. DDoS is one of the largest threads for the internet users & cloud service providers. Data integrity is necessary for any cloud data centre to avoid data corruption or data crash. Security is major dilemma in cloud environment.

In Proposed mechanism DDoS is detected & pre-empted by log monitoring of each & every request of services provided. Once attacker has been detected by log monitoring Attacker will be blocked permanently or tentatively depending on the log details. Mobile cloud user needs their data to be safe & private to maintain confidentiality. Data integrity can be achieved by implementing M-AES algorithm to the data stored in mobile cloud. M-AES algorithm preserves the data integrity in mobile cloud computing.

Question arises why combining DDoS & Data Integrity? After preventing DDoS attack providing upload & download data services to protect data stored on cloud servers from spoofing, data integrity is provided to data. If a user uploads data & malicious user or hacker tries to modify the data by spoofing in such cases, providing encryption to data before uploading data on cloud as well as by sending verification code to registered email-id as a security purpose. Keep log of file details like file size, date of upload, number of words, type of file by using these parameters spoofing can be detected.

General Terms

Security, One Time Password Generation Algorithm.

Keywords

Mobile Cloud Computing (MCC), Denial-of Service Attack (DoS), Distributed Denial of Service Attack (DDoS), Security, Data Integrity.

1. INTRODUCTION

Mobile cloud computing refers an infra where data servers & data filtering happens outside of mobile device. Moby cloud applications move data servers & computing power away from mobile device over wireless connection. Mobile device comes across to various resource challenges like battery power consumption, storage occupation & bandwidth consumption. Mobile cloud computing has many advantages to users like allowing them to use cloud platform, cloud infrastructure & software's provided by cloud at cheap price . Mobile cloud computing provides cloud users or clients to use data centers for storage purpose as well as services of cloud, must have the powerful system configuration like CPU speed, capacity of memory etc.

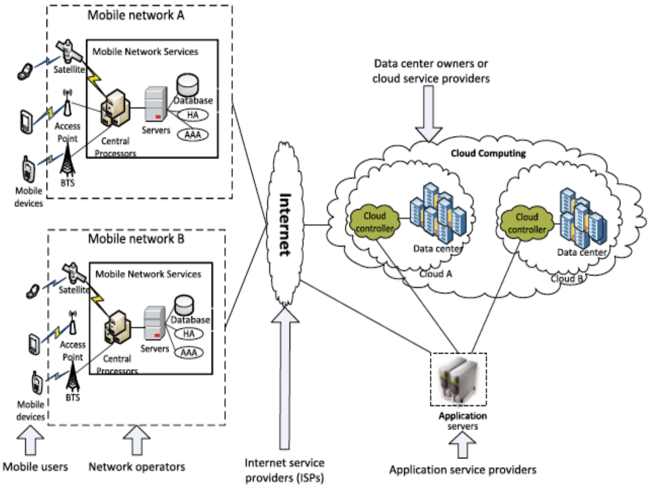


Fig. 1 MCC Architecture

Distributed Denial of service attack is a kind of Denial of Service (DoS) attack. The only difference between Denial of service attack & Distributed Denial of service attack is Denial of Service attack targets only a single user, a host computer & can be network whereas DDoS attack targets the larger websites or DNS server. In other words, DDoS attacker pre-empt the legitimate users from using the available services by flooding or by consuming available bandwidth. So that other users cannot be able to use the services or resources provided. At the time of DDoS detection need to consider the following parameters: CPU cycles, memory cycles, bandwidth & money [8]. Bandwidth is the only user resource server uses. Based on the mentioned parameters server should arrange resources or services so that if user has a fraction f of the user's total resources, that user can have a privilege to ask up to a fraction f of the cloud server. When the server is attacked, it endorses all the users to consume their bandwidth. So that other users will not be able to send service request.

Client requests for resources or services control system as shown in fig. 1 will first send a verification code on the specified e-mail ID. After authenticating the verification code legitimate user can use the services like upload & download. If it is found that the requesting client is malicious user trying to do DDoS attack will be blocked by the control system tentatively or permanently depending on the log monitoring system. And if it is a legitimate user then control system will allocate the requested resources to the client.

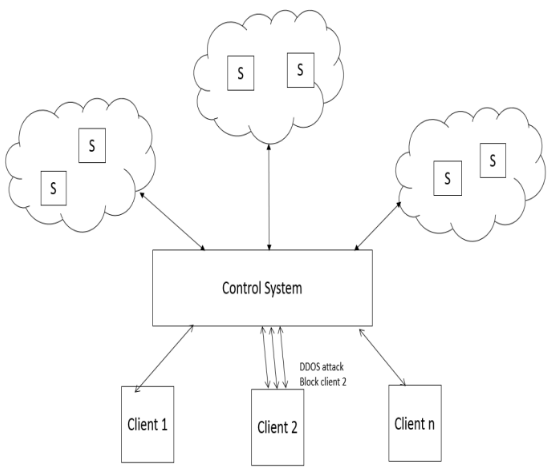


Fig. 2 DDoS Detection Block Diagram

Spoofing can be possible in mobile cloud due to security purpose providing Data Integrity to data stored in cloud servers or data centers. In proposed system data upload & download services are provided. If client uploads a file on cloud server & any malicious user or hacker tries to modify file contents. In such cases data integrity plays very important role by keeping log of each & every file with details like file name, size, number of words, type, date of file upload as well as if file modifies by the malicious user then date of modified file is also kept in records.

2. LITERATURE REVIEW

Some researchers proposed a system that dynamically allocates resources to attacking user called malicious user to detect DDoS attacker from available cloud customers. When a DDoS attack happens, simply allocate idle resource of the cloud to victim in order to quickly sorted out attack packets and assure the quality of the service for legitimate users simultaneously. This system needs to improve the M/M/m model to a general model, such as the M/G/m model. As well as we want to discover what should we do if a cloud data center runs out of resources during a DDoS attack [1]. When cyber-attacks and cyber interruptions happen, millions of users are affected & the associated security threats prevent this progression. Characteristics of our method and determining how an attack against the cloud's infrastructure would affect performance. New algorithms optimized for detecting cloud attacks in an efficient manner are needed, and this is something we will explore further [2]. Some author proposed system to allocate virtual machines to build side channels to extract private information from virtual machines on same servers [3]. Cloud computing is also suffering from some weaknesses like security & privacy, Internet Dependency, confidentiality, reliability, Availability, And Enterprise Applications Can't Be Transferred Simply. Author conclude that security is biggest hurdle in acceptance of cloud computing. Cloud service users are in fright of data loss, security, data reliability and availability issues. Developed application needs to be much secure, Identify Techniques to enhance resources along with better performance. To reduce the disadvantage of cloud computing and work to provide excellent services to the cloud user in cost effective manner [4]. Clients require their data to be safe and secure from any modifications or changes or unauthorized access in cloud computing. Various algorithms and protocols are applied by the various mechanisms of this archetypal to provide the maximum levels of integrity for data stored in public cloud for eg. Amazon S3. The major weakness of existing data integrity checking techniques is that they introduced privacy violation during integrity verification [5]. Some author discussed about what is cloud computing and the part of cloud storages centers in cloud computing, and describing the most important safety threat of cloud storages which is data integrity and data privacy or confidentiality, the proposed mechanisms for integrity assurance and the difficulties being faced in these mechanism. Security & privacy is a problem with rising security, the breaking points in security also occur. The mechanism author proposed can be implemented using much better encoding techniques so that the security rises more as well as data integrity enhances more [6]. Data protection & security is used to assure secure in communication, data storage and data broadcast. Security of hypermedia data is an imperative issue because of fast analysis of digital data uses the permutation step of Data Encryption Standard (DES) algorithm. Theoretical study and experimental results prove that this method provides high speed of encryption as well as rarer exchanges or transfer over unsecured network. Modified-AES algorithm is a fast and lightweight encryption cryptographic algorithm for security of multimedia data [7].

3. PROPOSED SYSTEM

Proposed system is divided into two main parts first is DDoS attack detection & prevention. Second is Applying data integrity on services provided like uploading & downloading Data from server.

3.1 Intrusion Detection & Prevention Mechanism

DDoS attack is detected by keeping log monitoring system. Below flowchart shows the DDoS detection & prevention.

In flow chart shown in fig. 3 whenever client request for service it has to first authenticate from control system after authentication control system will check for the intrusion pattern if it has found it is a malicious user control system will block the user for some period of time. And if the requesting client is legitimate user then grant the request by allocating requested resources or services. One more option for non-registered users is also available. Non-registered users can also upload or download data on cloud is also provided. And it is also possible that non-registered user can tries to do DDoS attack on cloud. Then detected malicious user will also be blocked for some period of time & if it is a legitimate user then grant the request by allocating requested resources or services.

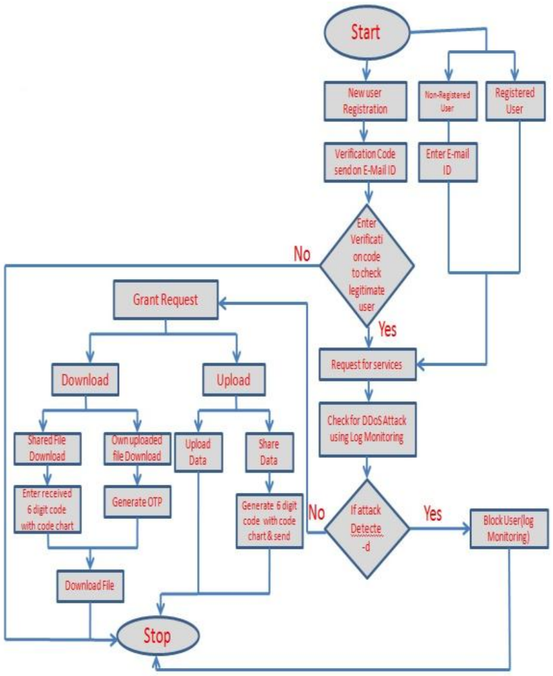

Start
New user Registration
Non-Registered User
Registered User
Verification Code send on E-Mail ID
Enter E-mail ID
Enter Verification code to check legitimate user
No
Yes
Grant Request
Request for services
Download
Upload
Check for DDoS Attack using Log Monitoring
Shared File Download
Own uploaded file Download
Upload Data
Share Data
Enter received 6 digit code with code chart
Generate OTP
Generate 6 digit code with code chart & send
No
If attack Detecte -d
Yes
Block User(log Monitoring)
Download File
Stop

Fig.3. Intrusion Detection & Prevention Mechanism

3.2 Attribute Sharing

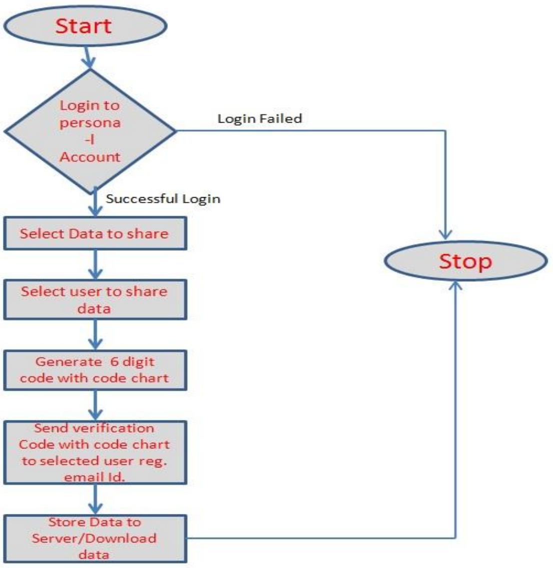

Start
Login to persona -l Account
Login Failed
Successful Login
Select Data to share
Stop
Select user to share data
Generate 6 digit code with code chart
Send verification Code with code chart to selected user reg. email Id.
Store Data to Server/Download data

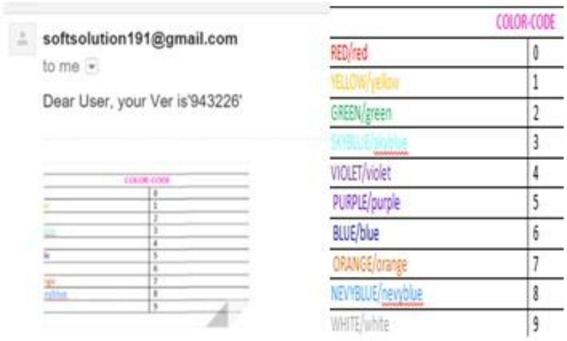
Fig. 4 Attribute sharing

After detecting legitimate user from malicious user to enhance the data integrity whenever legitimate user request for the data stored on cloud at the time of data storage owner of data will allocate attribute to the user with whom owner wants to share the data. So whenever users other than owner tries to access the shared data user has to enter the shared attribute to get the access after validation of attribute user can access the data. For further security owner stores encrypted data on cloud so that if an untrusted third party gets access to data will not be able to understand the stored data.

Proposed system to detect & prevent DDoS attack can be used by both registered & non-registered user. So there is possibility of happening or performing DDoS attack by any of the user like registered or non-registered. Now the question arises why there are two types of user like registered & non-registered? What is difference between registered & non-registered user? So the difference is that registered user can share files with other users registered on the application this feature is not available to non-registered user. Verification code plays very important role in registered user profile as without verification no registered user can be able to use the services of the cloud application.

Whenever user uploads data in cloud application whenever user wants to download that uploaded file user has to enter the six digit key which was shared with the user whenever user or client selects on download. So key is nothing but one time password which plays very important part in upload & downloads service of the proposed system.

Now the question arises what is shared attribute? Whenever registered user shares data or file with other registered users on cloud application. User or client with whom data is shared will receive a six digits code with code chart as show in fig. 5 below. User has to enter the initials of the corresponding digit. For example as given in figure below six digits code like 943226 user has to enter the corresponding initials like ‘wvsggb’. This is how shared attribute works.



softsolution191@gmail.com

to me

Dear User, your Ver is'943226'

COLOR-CODE	
RED/red	0
YELLOW/yellow	1
GREEN/green	2
SKYBLUE/skyblue	3
VIOLET/violet	4
PURPLE/purple	5
BLUE/blue	6
ORANGE/orange	7
NEVYBLUE/newblue	8
WHITE/white	9

Fig. 5 Shared Attribute

4. PERFORMANCE ANALYSIS

In this, we analyzed the performance of the proposed DDoS detection & prevention mechanism for DDoS mitigation in a cloud from varies approaches also analyzed the performance of Data integrity detection. Studies the performance of the existing proposed mechanisms like to prevent the DDoS attack some researchers used idle server allocation or two tiers CAPTCHA just to differentiate between robots from normal users & some used virtual machine allocation. DDoS can be detected using following parameters like CPU cycles, memory cycles, bandwidth & money. We are mainly focusing on bandwidth attack detection where attacker tries to target the cloud servers by flooding by consuming all their bandwidth so that no other user can use the services of cloud application.

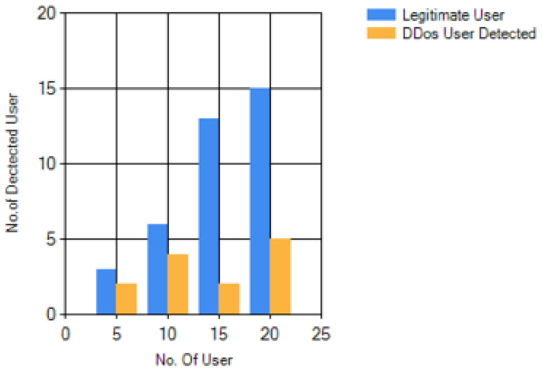


Fig. 6 Performance Analysis of DDoS Attack Detection

Considering graph shown in fig. 6, it shows the performance of DDoS attacker detected by using the proposed IDPS(Intrusion Detection & Prevention System) using following parameters like IP Address, host address, type of packet, time , counter to count number of request. If user exceeds the counter limit will be blocked by the IDPS system tentatively. Technically we cannot block DDoS attacker because if user is trying to open an website but server is busy as server is not available to fulfill the request asked by a legitimate user. In such cases we cannot block a legitimate user from accessing services of a developed application. We developed the machine learning scheme where number of legitimate users' verses number of DDoS detected user has been shown. Where no of legitimate users are more than number of DDoS attacker has been shown. For an example if there total fifteen users out of which five has been detected as a DDoS attacker.

Analyzed the performance of Data Integrity Detection which is applied on the data uploaded on cloud application. Studied the present proposed mechanisms like they just applied encryption algorithms to data in cloud like DES , RSA etc . In our proposed system we not only applied advanced encryption mechanism but also one time password mechanism to the services provided by cloud application. Data Integrity can be detected using various parameters like number of requests, buffer overflow & last but not the least file size. But we are concentrating mainly on number of requests to access the services like upload & download data or file from cloud application.

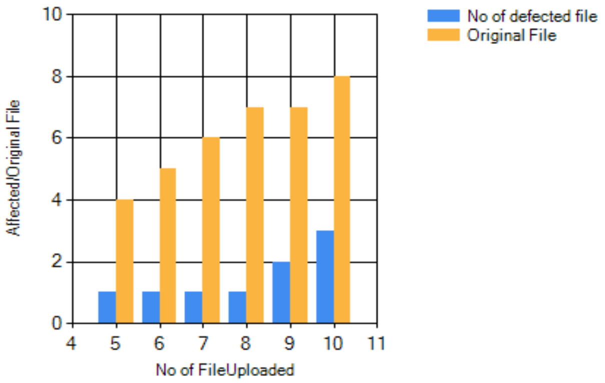


Fig. 7 Performance Analysis of Data Integrtity Detection

Considering graph shown in fig. 7, it shows the performance of the Data integrity detection using the proposed mechanism using following parameter like file type, number of words, file extension, file size, & number of characters in a file. Data integrity can be maintained, enhanced & detected only by using above mentioned parameters only. As we developed machine learning system where affected original file verses number of file uploaded has been shown. If there are 11 file uploaded among them 3 can be spoofed, hacked or modified by hacker or malicious user. This ratio is obtained by considering the above mentioned parameters only.

Table 1Comparative Analysis of Encryption Algorithms

Parameters	M-AES	DES	RSA
Key	128,192,256 bits	56 bits	1024 bits
Type of Algorithm	Symmetric	Symmetric	Asymmetric
Key Generation Time	Less	Less	More
Amount of Data	Large	Large	Small
Computation Time	Less	Less	More
Brute Force Attack	Not Possible	Possible	Not Possible

Above table 1 shows the comparative analysis of Cryptographic Encryption Algorithm. We are comparing the existing encryption technique with the one we are implementing in our Data integrity proposed mechanism. Till date DES & RSA encryption algorithms has been implemented. We are implementing M-AES in our proposed mechanism which take 128, 192 & 256 bits key. Whereas DES uses 56 bits key & RSA takes 1024 bits key. Brute force attack is not possible on large bits key like 256 bit key is large enough to avoid this of attack [7]. What exactly brute force attack is Brute force is a trial and error method to decode encrypted data like passwords or Data Encryption Standard (DES) keys, AES keys & RSA keys through obsessive effort (using brute force).

M-AES & DES are symmetric key algorithm & RSA is asymmetric key algorithm. Now question arises what is the difference between symmetric & asymmetric key algorithm. Technically symmetric key algorithm uses same key at the time of encryption & decryption of data. Whereas asymmetric key algorithm uses different keys at the time of encryption & decryption of data. M-AES takes less time to generate key as compared to RSA & takes more time as compared to DES encryption algorithm. Whereas DES takes less time to generate key as compared to both the encryption algorithm M-AES & RSA. And RSA takes more time to generate key as compared to both algorithms DES & M-AES.

M-AES & DES can be applied on large amount of data whereas RSA is applied on small amount of data. M-AES & DES takes less time to compute as compared to RSA encryption algorithm. Proposed mechanism uses 256 bits key to avoid brute force attack as well as it takes less computation time & can be applied on large number of data & also takes less key generation time as compared to RSA where RSA can be applied on small amount of data. And we cannot predict how much data user can upload on our cloud application. So we can conclude that M-AES is the best option as compared to existing mechanisms used.

5. CONCLUSION AND FUTURE WORK

In this paper we discussed the DDoS attack prevention mechanism which is associated with Data Integrity of the data uploaded on our cloud application. DDoS prevention & Data Integrity maintenance is combined for the first time ever. Why we are combining DDoS with data integrity together? As per our research we are providing services like upload data on cloud & download data form cloud. As data is involved it should be secured on cloud to maintain confidentiality & reliability of data we are appending Data Integrity to DDoS.

Also used One Time Password concept for downloading of self-uploaded data from cloud as well as shared attribute concept which is explained above is used for shared data with other registered users using shared attribute with colour code chart is also a new concept introduced.

Drawback of proposed mechanism is to implement it in time real time application. And evaluate the proposed application with large number of users like 100 or 1000 users at the same time to evaluate its performance.

6. REFERENCES

[1] Shui Yu, Yonghong Tian, Song Guo, and Dapeng OliverWu, Fellow ,"Can We Beat DDoS Attacks in Clouds?", IEEE TRANSACTIONS ON PARALLEL ANDDISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014.

[2] Aine MacDermott, Qi Shi, Madjid Merabti, and KashifKifiyat , "Considering an Elastic Scaling Model for Cloud Security", International Conference for Internet Technology and Secured Transactions (ICITST-2013)

[3] Yi Han, Jeffrey Chan, Tansu Alpcan, Christopher Leckie , " Using Virtual Machine Allocation Policies to Defend against Co-resident Attacks in Cloud Computing", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 2015

[4] Poonam Yadav, Sujata ," Security Issues in Cloud ComputingSolution of DDOS and IntroducingTwo-Tier CAPTCHA" , International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013

[5] Mohammed Faez Al-Jaberi and Anazida Zainal, "Data Integrity and Privacy Model in Cloud Computing", 2014 International Symposium on Biometrics and Security Technologies (ISBAST).

[6] Satyakshma Rawat, Richa Chowdhary & Dr. Abhay Bansal, "Data Integrity of Cloud Data Storages (CDSs) in Cloud", Rawat et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013.

[7] Luminiţa SCRIPCARIU and Mircea-Daniel FRUNZĂ, "Modified Advanced Encryption Standard", 11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 17-19, 2012.

[8] Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenker. DDoS defense by offense. In Proceedings of ACM SIGCOMM, 2006.

[9] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS‟07: Proceedings of the 14th ACM conference on Computer and communications security.

[10] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175,2008.

[11] Haiqin Liu and Min Sik Kim. Real-time detection of stealthy DDoS attacks using time-series decomposition. In Proceedings of IEEE International Conference on Communications 2010, May 2010.

[12] M. Guirguis, A. Bestavros, and I. Matta. Exploiting the transients of adaptation for RoQ attacks on internet resources. In Proceedings of IEEE ICNP, pages 184–195, Berlin, Germany, Oct 2004.

[13] Subashini, S. and V. Kavitha, A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011. 34(1): p. 1-11.

[14] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in SP '00: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2000, p. 44