***I.J. Wireless and Microwave Technologies*, 2019, 1, 43-51**
Published Online January 2019 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2019.01.05

***Available online at* http://www.mecs-press.net/ijwmt**

Design of Effective Security Architecture for Mobile Cloud Computing to Prevent DDoS Attacks

Kaushik Sekaran[a], G.Raja Vikram[b], B.V. Chowdary[c]

[a,b,c]*Associate Professor, Vignan Institute of Technology & Science, Hyderabad, Telangana, 508284, India*

Received: 07 August 2018; Accepted: 22 October 2018; Published: 08 January 2019

Abstract

A DOS (Denial of Service) attack, as its name suggests, denies or blocks access to certain services by flooding either the bandwidth of a specified network or by targeting its connectivity. There are much security challenges in mobile cloud computing. Cloud indicates a period of the computing where the services, which are an application, are made available by the internet. Cloud based computing is very adjustable and cheap as to providing a platform for various IT services. The mobile systems can hinge on the cloud based computing with mobile agents and can undertake various processes such as the searching or storing, etc. While it's very economic, it has many challenges such as the security. Various researches have been carried out to build a secure mobile cloud based computing. In this paper, we have viewed and analyzed the DDOS (Distributed Denial of Service) attacks in depth to prevent it in the mobile cloud computing.

Index Terms: Mobile Cloud computing, distributed denial of service (DDOS) attacks, security challenges, searching, cloud based computing, Mobile Agents.

1. Introduction

Mobile cloud based computing is a type of varying technology of computing. It involves development on side-by-side processing and grid wise as well. It basic concept involves instinctive split of a large section of a program based on calculation into various very small subroutines with help of a network and is further handed to the operating system of several servers. After all the calculations part and analyzing, it will forward the result to the respective user. It has a security issue for the mobile devices that are restricted to some specified resources.

* Corresponding author. Tel.: +91-8015628957
E-mail address: drkaushiksekaran@gmail.com

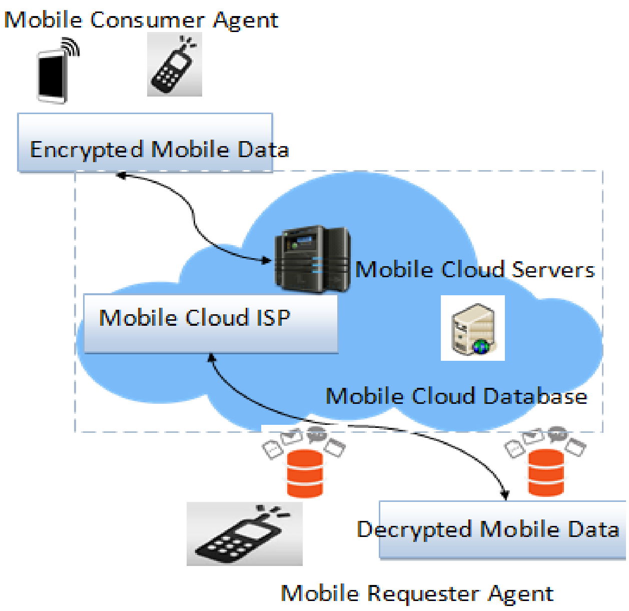

Fig.1. Effective Security Architecture For Mobile Cloud Computing

Fig.1, represents the effective security architecture for mobile cloud computing. Generally, in the mobile cloud computing, five important components are there to understand about the mobile cloud computing security architecture. They are;

- Mobile Consumer Agent
- Mobile Cloud Service provider
- Mobile Encrypted/Decrypted data
- Mobile Requester Agent
- Mobile cloud databases

In our proposed effective security architecture for mobile cloud computing, we have worked clearly on the application layer of the cloud services from the Mobile Cloud Service provider. Initially, the Mobile Consumer Agent would login into the cloud data centers by providing the proper credentials and start accessing the mobile data through various mobile cloud databases. All the data shared towards the mobile cloud environment will be having much security such as high level encryption and decryption processes. But still, in the mobile cloud computing, we have lot of security flaws like flooding of the HTTP/TCP packets that leads to DDOS attacks possible in the mobile cloud computing environment. In order to prevent these DDOS attacks, a proper methodology and algorithm is needed in the router and the cloud servers. Our proposed work aims in giving better security against the DDOS attacks.

1.1 Existing Methodologies for DDoS attack detection in MOBILE cloud computing

1.1.1 SYN cookies method

This is considered as the most efficient method against the SYN flood attacks. In this method the server stores the authentication information in the sequence in SYN/ACK packets instead of storing in the backlog queue. When the victim server is replying to a request it uses a formula to calculate the sequence number of the SYN/ACK packet. Cookie value is hash of source port, source address, destination port, destination address, maximum segment value stored in SYN, a minute counter and a secret value that is different for each server boot. On receiving a request the server [1] verifies the cookie then only a connection is established. It is compatible with all TCP implementations. The server however cannot resend a lost packet as information becomes unavailable. Computation of hash function also consumes lots of resources.

The architecture includes secure overlay tunneling, routing via consistent hashing and filtering. They reduce the probability of successful attacks by performing extensive filtering near protected network hosts, pushing the attack point into the network core, where high-speed routers can handle the extent of attack traffic and introducing some kind of randomness and anonymity into the architecture, making it difficult for an attacker to target some nodes along the path to a specific SOS-protected host. Using simple analytical models, we evaluate the probability that an attacker can successfully launch a DDoS attack against an SOS-protected network. The analysis suggests that such architecture reduces the probability of a successful attack to small levels. The performance measurements using a prototype implementation indicate an increase in host to host latency by a factor of two for the any case, and an average heals time of less than ten seconds.

1.1.2. Probabilistic packet marketing (PPM)

While analyzing the probabilistic packet marketing (PPM) [2] suggested that the 64 bits comprised of 32 bits internet protocol physical address of the router together with 32 bits hash of the router's IP address should be split into 8 equal parts. Each packet stores the edge value. Once the victim has collected ample amount of dangerous packets, the reconstruction program combines the edge values using the fragment ID and the path. Hence it constructs the attack path. This technique doesn't itself stop the DDoS attack; they just determine the edge network having the attacker. Dynamic filters could be deployed close to the identified sources. As the malicious packets aren't marked in this technique, the attacker may send spoofed marking fields and impede trace back. It can't trace true source of reflector DDoS attacks. If the attacker sends packets of size larger than maximum transmission unit size the technique is paralyzed.

1.1.3. DDoS Parallel Attack Diagnosis

DDoS parallel attack scheme [3] hinges on and generalizes the IP traceback schemes to obtain the information concerning whether a network host is on the attacking path of an attacker (infected) or not (clean). They observe that, while an attacker will have all the hosts on its path marked as infected, hosts on the path of a proper client will mostly be clean. By preferentially filtering out packets that are marked with the marks of infected edges, the proposed scheme eradicates most of the DDoS traffic while affecting legitimate traffic only slightly. Simulation results based on real-world network structures all demonstrate that the introduced technique can improve the flow of legitimate traffic by three to seven times during DDoS attacks.These techniques are based on packet marking and Pushback. In these techniques the routers embed port identifiers on which the traffic towards victim server is received. Every input interface has a unique identifier, PID. The 17-bit IP packet is divided into: 5- bit hop count, 6- bit PID and 6- bit XOR field. This way, tracking of only one attacker is possible at any moment. PAD method is an improved form in which multiple attackers can be tracked. The most important benefit of these methods is that they don't require universal deployment. It is although pretty expensive as all routers need to do ADMM and PADMM until the attacker is determined.

2. Related Works

Lee et al. [4] suggested the use of Distributed Change-point Detection (DCD) design to build a change aggregation tree so as to detect attack in early stage. In this several autonomous systems should work in synchronization and each AS should designate a CAT to do this. At the base layer, each border router acts as a sensor so as to monitor local traffic fluctuations. In case of an attack, an alarm is triggered by the routers and a report is sent to the CAT servers at the center. The CAT server then makes a subtree according to the reported anomaly. The CAT servers contact with each other via VPNs. All the servers dispatch the generated subtree to CAT server of the domain, which acts as a root. This mechanism is able to detect attacks very quickly but may inflict an enormous overhead for some routers. Routers should compare computed DFA parameter with the reference parameter (B). It needs a dedicated server at all times to calculate B.

Agarwal et al. [5] considered recursive pushback of max–min fairness rate limits, beginning from the overloaded routers to the upstream routers. In this technique an aggregate congestion control identifies the traffic in the router level and prepares the attack signature that can be translated by the router filters. A traffic aggregate is defined as a group of flow having some common properties. The congested router asks the adjacent router to set a rate limit on the aggregate. The receipt routers recursively transmit pushback further upstream. It effectively mitigates DDoS attacks [14] when attacking machine are gathered in few places. It is not that effective if the attackers are extensively distributed throughout the network. It also hurts some innocent servers also.

Yaar et al. [6] considered DDoS attacks as a resource management issue and suggested to dispense the resources of the victim server in a max–min fashion between level-k routers. Jin et al. [7] introduced the Hop Counting Packet filtering method built on noting the values of time-to-live (TTL) of packets. The victim checks the determined TTL of a packet. It then estimates the value of the initial TTL that the sender placed in the packet. The operating system uses few of these values, which facilitate accurate guesses. The hop count is calculated as the difference between the initial TTL value and the observed TTL value. Under normal circumstances the victim server maintains a table of the regular legitimate clients and the corresponding hop counts. During the time of attack the packets that are missing from the table or have hop counts not matching their source address are labeled as spoofed. Legitimate clients succeed in establishing a connection with the server. For the generation of fingerprint each router assigns an n-bit secret random number to each of its network interfaces. The fingerprint has two fields: a d-bit distance, denoting number of intermediate routers and an n-bit path id, denoting identifier derived from random numbers. It is effective only against direct DDoS attacks. It is cost effective as compared to HCP as it uses hash operations to embed the information in the packet. The paper uses IP identification field of 16- bits to embed the fingerprints. Addition of fingerprint decreases the overall speed.

The work by [12] discusses the various aspects of mobile cloud based computing and its importance in every way. It also highlights the issues which most of the providers of cloud are looking into as to enhance the performance by securing the integrity of the data. To conclude, it gives a detailed study on the various issues of the mobile cloud. The paper [13] takes into consideration the various architectures of the mobile based cloud. Computing and its various characteristics and also the security issues it faces. It also looks into the various measures that can be taken to resolve the issue. The various measures that can be opted are putting authentication checks of the user which prevents the system from getting hacked. The paper [8] gives an insight about what is mobile cloud based computing and its proper definition. The capabilities of the mobile devices regarding the interactivity and availability. It also discusses the various security problems that the mobile system has and how other authors have explained it taking into consideration the various aspects such as the model, its combination and device processing. It is basically a survey which explains the various security issues.The paper [9] includes the basic definition of mobile cloud computing and the different types of applications available for mobile devices such as the web and hybrid app to name a few. It also gives a detailed explanation of computing technology and various types of cloud services and also insight into the security issues.

The paper [10] discusses the various issues related to security, the advantages of mobile cloud and the trends that have emerged in the industry. And mainly focuses on the mobile cloud based computing. It discusses the advantages such as how the user can use the various infrastructures and evolves and makes use of storage spaces. It gives a major set of solution for the issues related to security such as the insertion or the deletion of the block and updating of the file on the cloud. The paper [11] gives an insight about the latest trends in mobile computing and also the security related risks and issues that a mobile system has. Taking in consideration the various security issues, it also provides the various types of solutions such as the protection of identity using the devices which are embedded and the access to cloud to be protected.

3. Proposed Methodology for DDoS Attack Detection in MOBILE Cloud Computing

By considering various security issues, the mobile cloud computing need much protection from the vulnerable devices. To identity using the devices which are embedded and have the access to cloud need to be protected. Also, the main security issues highlighted in any works are the privacy, the integrity methods and the availability of the data and the various issues related to the data taking in the mobile cloud based computing. Our proposed Methodology for DDoS attack detection in mobile cloud computing have been analyzed and made as an algorithmic view for implementing it on any router or cloud data center in any cloud industry.

3.1 Algorithm for DDoS attack detection in MOBILE cloud computing

Acronyms

- **MCS-** mobile cloud server
- **CDC-SP -** Cloud data center- Service Provider
- **M-ID-** Mobile Identity

Our proposed Algorithm for DDoS attack detection model involves three

Steps:

- ✓ *Generation of M-ID in MCS*
- ✓ *Encryption of Mobile data in MCS*
- ✓ *Decryption of Mobile data in CDC-SP*

1. *Generation of M-ID*

Before the data is encrypted, mobile ID generation must be done by the mobile Cloud server

2. *Let K be a pseudorandom function, letm_p be a pseudorandom permutation and let CH bea cryptographic hash function.*

Generate $m_p(k) = (CH(K), g)$ and $m_p(ID) = (CS, CH(K))$, such that

$CH(K) \equiv 1(\mathrm{mod}\ m_p\ 'K')$, K is a large secret prime such

that $K > \lambda$ and $CS > \lambda$, m_p (k) is a generator of M-ID

Output in M-ID $CH\{(m_p\ (k))\}$ results in detecting intruders(flooders) in MCS.

4. Results and Performance Evaluation

In Mobile Cloud computing environments the encryption analysis is one of the important factor that could be done by creating comprehensive model in any tool to understand about the actual reduction of response time in the cloud data centers. We have used dynamic cloudsim tool to configure and analyse our results. Assume there are three mobile cloud servers located in an organization. Now our testing scenario in dynacic cloud sim is all the mobile agents have attacked by DDoS such as initial GET request and HTTP request of independent nodes is assumed to have more vulnerability.

We are introducing an even analysis model table and graph to understand this scenario. From table 1 we could clearly understand about the given scenario in mobile cloud servers. From the results, we can able to understand the cloud encryption time is being reduced after implementation of our proposed algorithm and that has been depicted in the figures 2.

4.1 Simulation setup and metrics

4.1.1 Packet loss Analysis

The simulation results shows that the loss of packets (HTTP GET) while DDoS attacks in security breach towards Mobile cloud servers. During the normal time the HTTP packet loss is near about small and at the time of attack it goes very high. It is depicted towards the graph in the figure 3.

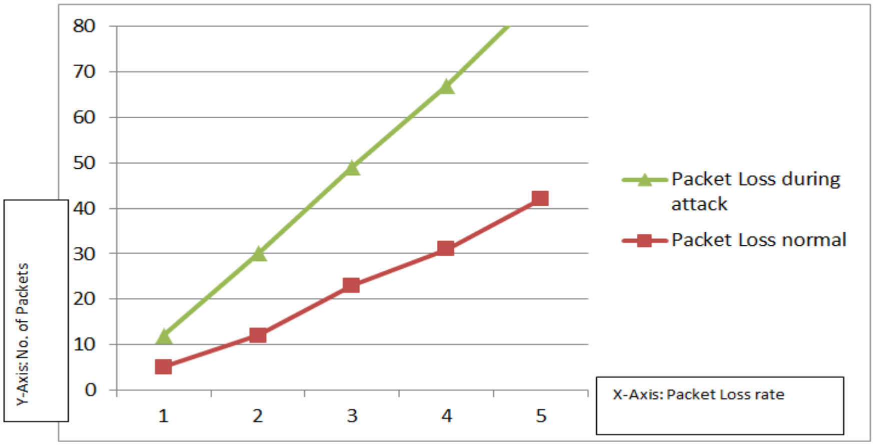

Fig.2. Packet Loss Analysis in DDoS enabled mobile cloud computing

4.1.2 Throughput Analysis

During DDoS attacks always the throughput decreases due to the heavy congestion in network. The simulation results and graphs in figure 4 represents after applying our proposed algorithm the throughput increases. Also, our model has been compared with IDS (Intrusion Detection system) model, and we have better results.

Table 1. Throughput Analysis

No. of Packets	Throughput during attack - Proposed model	Throughput during attack - IDS model
10	50	40
20	67	33
30	71	56
40	89	70
50	107	85

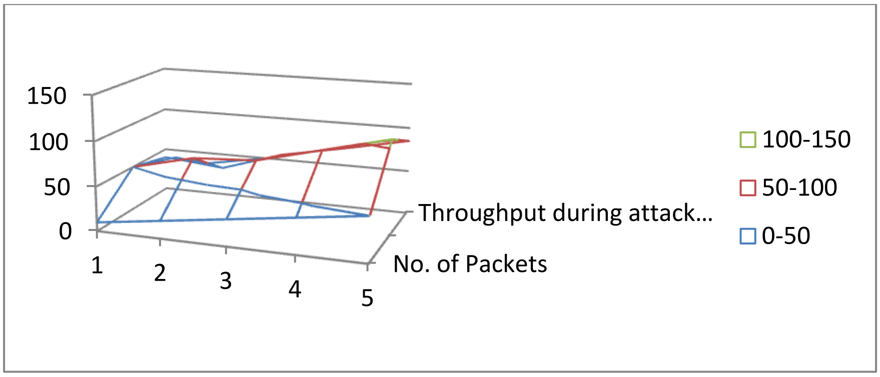

Fig.3. Comparison of Throughput Analysis in DDoS enabled mobile cloud computing

5. Conclusions

The mobile cloud based computing is a new venture since a long time and is still developing. The issues of security and privacy that can be found in it are a result of cloud based computing. However, such issues cannot easily be resolved because of the issue of various constraints that are there on the mobile systems related to storage space, processing speed, etc. To resolve such issues a concrete framework needs to developed which can tackle the various constraints on the mobile systems and also privacyof user is maintained simultaneously keeping in the consideration its cost-effectiveness and networks.

References

[1] Hunter, P. (2003). Distributed Denial of Service (DDOS) Mitigation Tools.*Network Security*, *2003*(5), 12-14.

[2] Beitollahi, H., & Deconinck, G. (2012). Analyzing well-known countermeasures against distributed denial of service attacks. *Computer Communications*, *35*(11), 1312-1332.

[3] Lee, K., Kim, J., Kwon, K. H., Han, Y., & Kim, S. (2008). DDoS attack detection method using cluster analysis. *Expert Systems with Applications*,*34*(3), 1659-1665.

[4] Agarwal, S., Dawson, T., Tryfonas, C. (2003). DDoS mitigation via regional cleaning centers. Sprint ATL Research Report RR04-ATL-013177.

[5] Yaar, A., Perrig, A., & Song, D. (2004, May). SIFF: A stateless Internet flow filter to mitigate DDoS flooding attacks. In Security and Privacy, 2004.Proceedings. 2004 IEEE Symposium on (pp. 130-143). IEEE.

[6] Y. Chen, K. Hwang, W.-S. Ku, Collaborative detection of DDoS attacks over multiple network domains, IEEE Transactions on Parallel and Distributed Systems 18 (12) (2007) 1649–1662.

[7] L. Feinstein, D. Schnackenberg, R. Balupari, D. Kindred, Statistical approaches to DDoS attack detection and response, in: Proceedings of DARPA Information Survivability Conference and Exposition, Washington, DC, USA, 2003, pp. 303–314.

[8] A.L. Toledo, X. Wang, Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks, IEEE Transactions on Information Forensics and Security 3 (3) (2008) 347–358.

[9] P. Ferguson, D. Senie, Network ingress filtering: defending denial of service attacks which employ IP source address spoofing, internet RFCs RFC 2827, 2000, pp. 1–10.

[10] K. Park, H. Lee, On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets, in: Proceedings of ACM SIGCOMM, San Diego, California, USA., 2001, pp. 15–26.

[11] Soeung-Kon(Victor) Ko, Jung-Hoon Lee, Sung Woo Kim, Mobile cloud computing security considerations, January 2012.

[12] Sekaran Kaushik and P. Venkata Krishna. "Big Cloud: a hybrid cloud model for secure data storage through cloud space." International Journal of Advanced Intelligence Paradigms 8, no. 2 (2016), pp. 229-241.

[13] Sekaran, K., & Krishna, P. V. (2017). Cross region load balancing of tasks using region-based rerouting of loads in cloud computing environment. International Journal of Advanced Intelligence Paradigms, 9(5-6), pp. 589-603.

[14] Sung, M., Xu, J. (2003). IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks. IEEE Transactions on Parallel and Distributed Systems, 14(9), pp. 861-872.

Authors' Profiles

Dr. Kaushik Sekaran currently working as Associate Professor in Dept of computer science and engineering, Vignan Institute of Technology & Science, Hyderabad, Telangana, India. His main thrust research areas are Cloud Computing, IoT and Fog computing. He has 12 published papers in reputed SCI and Scopus indexed journals, conferences, book chapters and books. He is guest editor/reviewer for various International Journals. Kaushik Sekaran received his Bachelor of Technology in Computer Science and Engineering from SASTRA University, Thanjavur in the year 2005. He then pursued postgraduate studies and received his Master of Engineering degree (in Computer Science and Engineering) from Mepco Schlenk engineering college, Affiliated to Anna Univesity, Chennai in the year 2008. From March 2009 to April 2017, for the period of 8 years, he worked as an Associate Professor in School of computing science and Engineering at VIT University, Vellore, India. He finshed his Ph.D studies in the year 2015 in VIT University in the area of cloud computing. His current research interests include in the areas of cloud computing, distributed and Internet systems, overlay systems and applications, and Security issues in Peer-to-peer Networks.

Prof. Raja Vikram currently working as Associate Professor in Dept of computer science and engineering, Vignan Institute of Technology & Science, Hyderabad, Telangana, India. Raja Vikram is presently pursuing Ph.D from JNTU-Hyderabad. He received his Master's Degree in Computer Science & Engineering from JNTU-H. His research areas include Network Security and Information Security, Wireless Sensor Networks, Distributed Computing.

Prof. B V Chowdary currently working as Associate Professor in Dept of computer science and engineering, Vignan Institute of Technology & Science, Hyderabad, Telangana, India. B V Chowdary received his Master's Degree in Computer Science & Engineering from Dr.M G R Educational & Research Institute,Chennai.His research areas are Data Mining and Information Security.

How to cite this paper: Kaushik Sekaran, G.Raja Vikram, B.V. Chowdary, "Design of Effective Security Architecture for Mobile Cloud Computing to Prevent DDoS Attacks ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.9, No.1, pp. 43-51, 2019.DOI: 10.5815/ijwmt.2019.01.05