AN EFFİCİENT APPROACH USİNG DİFFİE - HELLMAN KEY EXCHANGE TO PROTECT CLOUD FROM INTERNET ATTACKS

Lokashree S[1], Lokana S[2]

[1,2]*PG Student, Rajeev Institute of Technology, Hassan*

ABSTRACT

Because of rising threat of internet attacks especially denial-of-service attacks traceback problem is often relevant to internet security. It is a problem that involves identifying the source of the attack packets. Because of the dynamic nature of cloud there is a new area of research called cloud forensics. The cloud forensics is the branch of forensics that applies computer science knowledge to prove digital artifacts. The Distributed Denial of Service (DDOS) is a widely used attack in cloud environment. Web services can get exposed to denial of services or xml denial of services attack that hamper web services by crashing the service providers and their services. To perform forensics of DDOS if it is identified using possible detection and prevention mechanisms then it would result in cloud forensics solutions and evidence collection and segregation. In order to address the problem of kinds of internet attacks against cloud web services there is a need to differentiate the legitimate and illegitimate messages. Proposed work has been used to not only trace DDoS attacking packets but it also enhances filtering attacking traffic. We have used three types of filters namely MATCH, MARK, MAKE OVER and DUMP[13]. Then we use DIFFIE-HELLMAN KEY EXCHANGE algorithm to protect the genuine/legitimate data. The DIFFIE-HELLMAN KEY EXCHANGE algorithm will encrypt the plaintext data into cipher text and then hides the message being exposed to the attacker. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. It focuses of three major security concerns: authentication, key generation and encryption of data.

Keywords: Traceback, Xdos Attack, Ddos Attack, Filters, DIFFIE- HELLMAN KEY EXCHANGE Algorithm.

I. INTRODUCTİON

In recent days Internet is being widely used for various activities, because it provides relevant information and important services in almost all fields such as educational, commercial , business, finance, hospitality, retail, entertainment, telecommunication, etc. Hence, it is very necessary to provide security to the internet users about their information and service provider, who provides service to them for their request in Cloud environment. Due to the interruption of service provided by service provider, inconvenience is caused to the cloud users. These interruption activities are due to Denial of service (DoS) \ XML denial of service (XDoS) attacks which done by the attacker for the material gain access or popularity or personal reasons [20]. Since the DDoS and XDoS attackers spoof the source address, tracing them is very difficult. DDoS attacks actually hamper web

services by crashing the service provider and its services. The proposed approach is very simple to implement, scalable enough and helps rescue from DDoS attacks more effectively since these attacks can only be detected and cannot be prevented. This approach uses DIFFIE-HELLMAN KEY EXCHANGE algorithm to encrypt/hide the original data being exposed to the attacker and establishes a shared secret key that can be used for secret communications while exchanging data over a public network. It uses two keys: one secret and other private key. If Sender wants to communicate with the receiver, he encrypts the message with his private key and senders' public key[21].

1.1 Characteristics of Cloud

- Individual use on request: A user can use his desired resources at any place and at any time through the global network without any conflict.
- Wide range of network accessing capacity: Capacities of the system are available to customers via a network and it can be accessed from various devices such as desktop, laptops, mobile phones, tablets, etc.
- Resource allocation: Simultaneous users can access the cloud resources at any time without any conflict. Cloud solutions have right to chose where the users data will be stored and processed.
- Elasticity and flexibility: Cloud dynamically allocates necessary resources, and resources are automatically restored to its original condition. The user is free to purchase additional resources and opportunities in any quantity and at any time.Pay per use: Cloud services are measurable and their usage is transparent, both for the service provider and clients.

1.2 Security Concerns

Trustworthiness is one of the key concerns of the cloud service provider. Organizations are carefully deceiving both their sensitive and insensitive data to cloud to fetch required services. Cloud works on pay per use basis. Suppose a DoS attacker intentionally sends numerous requests to cloud then the owner of that particular cloud will have to process more requests at a time. Meanwhile, if other genuine users sends request to the server on cloud, their service will be denied since the server will be busy serving the DoS attacker. The other worst case is DDoS attack, where the attacker compromises some more hosts to send the flood request.

1.3 Denial-Of-Service Attack/ Distributed Denial-Of-Service Attack

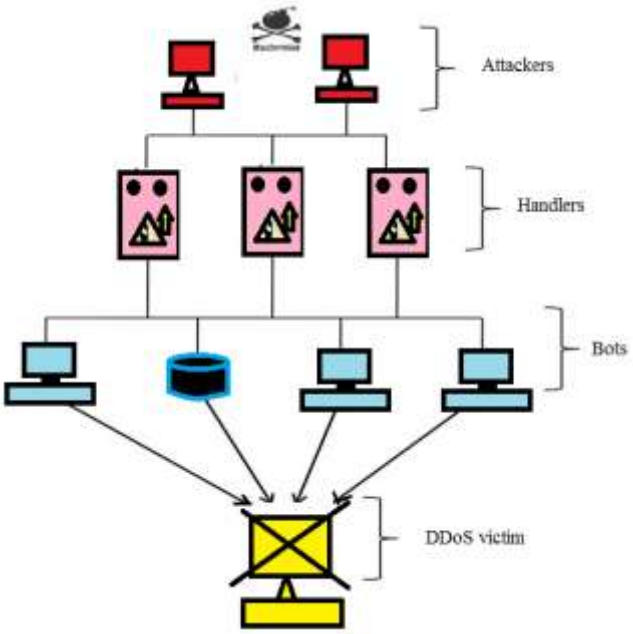
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. This attack hamper web services by crashing the service provider and its services.

1.4 Modes of Attack

In a denial-of-service attack, the attacker makes an explicit attempt to prevent legitimate users of a service from using that service.

Two common forms of DoS attacks are:

1. those that crash services and
2. those that flood services.



II. RELATED WORK

In a Cloud computing environment, cloud servers that provide requested cloud services, may sometime crash after they receive huge amount of request [16]. This situation is called Denial Of service attack. Cloud Computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. Cloud Computing is changing the IT delivery model to provide on-demand self-service access to a shared pool of computing resources (physical and virtual) via broad network access to offer reduced costs, capacity utilization, higher efficiencies and mobility. Recently Distributed Denial of Service (DDoS) attacks on clouds has become one of the serious threats to this buzzing technology. Distributed Denial of Service (DDoS) attacks continue to plague the Internet. Distributed Denial-of-Service (DDoS) attacks are a significant problem because they are very hard to detect, there is no comprehensive solution and it can shut an organization off from the Internet. The primary goal of an attack is to deny the victim's access to a particular resource. In this paper, we want to review the current DoS and DDoS detection and defence mechanism.

The main problem faced in a cloud environment is the Distributed denial of service (DDoS) [17]. During such a DDoS attack all consumers will get affected at the same time and will not be able to access the resources on the cloud. All client users send their request in the form of XML messages and they generally make use of the HTTP protocol. So the threat coming from distributed REST attacks are more and easy to implement by the attacker, but such attacks are generally difficult to detect and resolve by the administrator. So to resolve these attacks we introduce a specific approach to providing security based on various filters. We make use of five different filters which are used to detect and resolve XML and HTTP DDoS attack. This allows the security expert to detect the attack before it occurs and block or remove the suspicious client.

Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks [18]. DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not

obeying traditional end-to-end congestion control, the problem must be handled by the routers. Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack.

Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router's resources be used to route legitimate traffic. In this paper we present an architecture for Pushback, its implementation under FreeBSD, and suggestions for how such a system can be implemented in core routers.

Cloud Computing is an emerging area nowadays. Researchers are working on all aspects of cloud viz [19]. cloud network architecture, scheduling policies, virtualization, hypervisor performance scalability, I/O efficiency, data integrity and data confidentiality of data intensive applications. The dynamic nature of cloud presents researchers new area of research that is cloud forensics. Cloud Forensics is the branch of forensics for applying computer science knowledge to prove digital artifacts. The DDOS is the widely used attack in cloud environment. To do the forensics of DDOS if it is identified a possible detection and prevention mechanisms would aid in cloud forensics solutions and evidence collection and segregation. This paper presents different types of DDOS attack at the different layers of OSI model with increasing complexity in performing attack and focuses more on prevention and detection of DDOS at different layer of OSI and effect of DDOS in cloud computing.

The theoretical background of our proposed work is taken from reference [13]. We are giving security to the confidential data by using DIFFIE- HELLMAN KEY EXCHANGE algorithm. Diffie-Hellman key exchange approach uses two types keys: one is secret key and the other is private key. Sender communicates with the receiver by encrypting the message with his private key and senders' public key.

III. PROPOSED WORK

Flaws either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched. Of the kinds of network attacks, denial-of-service flood attacks have caused the most severe impact. Cloud computing suffers from major security threat problem by HTTP and XML Denial of Service (DoS) attacks. The combination of HTTP and XML messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider is called as HX-DoS attack. To address this issue, there is a need to differentiate the genuine or legitimate message and illegitimate message.

HX-DoS attack involves an attacker who compromises a client having an account to access the cloud service provider server. Therefore, the attacker gets direct connection through the system. Then the attacker will install HX-DoS attack program at the user end and initiates it. The XDoS attack can take place in few ways: First, a network can be flooded with XML messages (instead of packets), in order to prevent legitimate users to network communication. Next, if the attacker floods the web server with XML requests, it will affect the availability of these web services. Finally, attackers manipulate the message content, so that the result web server gets crash. In order to differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH filter. MATCH filter is located one hop away from host. The rule set of MATCH filter has been built up over time to identify the known HDoS and X-DoS messages. The well known HX-DoS attack is XML injection or XML Payload Overload, MATCH filter is trained and tested to identify these known attacks. After the detection of HX-DoS message, MATCH filter drops the packet which matches the rule set. The packets are subjected to marking after they are examined by the MATCH filter. The DIFFIE-

HELLMAN KEY EXCHANGE algorithm is used to convert the plaintext data into corresponding cipher text so that the attacker cannot view the original data being transmitted. Diffie–Hellman key exchange technique is accomplished by two parties who have no prior knowledge about each other to together establish a shared secret key over a channel.

IV. DESIGN CONSIDERATIONS

Consider two legitimate users and an attacker. User sends data through three filters namely, MATCH filter, MARK filter and MAKE OVER and DUMP filter to the server.

The message will be identified and if it is from an attacker then that message will be dropped before it reaches the server.

Modulo packet marking consists of two routers:

1. Edge router
2. Core router

On the victim side, by the time the victim starts collecting marked packets, all routers in the network will already have invoked the packet marking procedure. In extension, the victim does not have any knowledge about the real network or the attack graph. But the victim only knows the marking probability that the routers use.

It is appareled with the ability to mark packets as in the original Probabilistic Packet Marking(PPM) algorithm where each router shares the same marking probability. In specific, a router can either be a transit router or a leaf router. A transit router is a router that forwards traffic from upstream routers to its downstream routers or to the victim, whereas a leaf router is a router whose upstream router is connected to client computers and not to routers and forwards the clients' traffic to its downstream routers or to the victim. Assuredly, the clients are mixed with genuine as well as malicious parties. Likewise, every router will be having only one outgoing route toward the victim named "outgoing route toward the victim" and this can be further justified by the fact that modern routing algorithms favor the construction of routing trees.The plaintext data inside the packet will be converted into cipher text data using DIFFIE- HELLMAN KEY EXCHANGE algorithm so that when an attacker tries to get the data, he will be unable to read the original plain text data.

4.1 Goals

The denial-of-service (DDoS) attacks are addressed, where they try to suspend services of a host connected to the internet. The major goal of this project is to filter the genuine message from the message and pass that genuine message to the server, so that only genuine user can get resources of Cloud server. And the DIFFIE-HELLMAN KEY EXCHANGE algorithm is used so that the raw data is encrypted and is converted to cipher text so as to make it difficult the attacker to identify the message.

4.1.1 Cryptographic Explanation of Diffie-Hellman Key Exchange Algorithm [29]

The simplest and the original implementation of the protocol uses the multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p. Here is an example of the protocol, with non-secret values, and secret values[29].

1. Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $\boldsymbol{a} = \mathbf{6}$, then sends Bob $A = g^a \bmod p$

- $A = 5^{\mathbf{6}} \bmod 23 = 8$

3. Bob chooses a secret integer $\boldsymbol{b} = \mathbf{15}$, then sends Alice $B = g^{\boldsymbol{b}} \bmod p$
   - $B = 5^{\mathbf{15}} \bmod 23 = 19$
4. Alice computes $\boldsymbol{s} = B^{\boldsymbol{a}} \bmod p$
   - $\boldsymbol{s} = 19^{\mathbf{6}} \bmod 23 = \mathbf{2}$
5. Bob computes $\boldsymbol{s} = A^{\boldsymbol{b}} \bmod p$
   - $\boldsymbol{s} = 8^{\mathbf{15}} \bmod 23 = \mathbf{2}$
6. Alice and Bob now share a secret (the number **2**).

4.2 Modules

In a DDoS attack, an attacker compromises a client who has an account to access the cloud service provider server. By this way they get a direct connection through the system. The attacker then installs the DoS attack program at the user end and initiates it. To differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH. MATCH filter is located one hop away from host. MATCH's rule set has been built up over time to identify the known DDoS messages. With the help of known DDoS attacks like XML injection or XML Payload Overload, MATCH filter is able to be trained and tested to identify these known attributes. Upon detection of DDoS message, MATCH filter drops the packet which matches the rule set. After MATCH examines all the packets, they are subjected to marking.

Next marking scheme is the Mark algorithm. As the packets travel via network, they are marked with router information using modulo technique. Upon trace-back request, reverse modulo is used to make over the path traversed by the packets. The marking is done on both edge and core routers. When an edge router decides to mark an incoming packet, it fetches the code to be marked that corresponds to physical address of the host from the lookup table and encodes it into the packet. The edge router requires one bit for indicating whether the packet is marked or not and few bits for marking code and it maintains a lookup table called MAC to ID table, which has physical address of the hosts attached to the network and equivalent numeric code for each of the physical addresses.

The core router marks the packet only if that packet has been already marked by the edge router. Else, it would simply forward the packets. Core router maintains a table called MAC to Interface which contains the physical addresses of all of its hardware input interfaces and link numbers assigned to each of these interfaces.

When a router decides to mark, it consults the table to find the link number assigned to the inbound interface. The core router uses the modulo technique for marking is calculated as in Equation 1,

New marking information= current marking information × number of interfaces on the router + the link number (1)

Make over and Dump filter, which is built from the IDP and its location is one hop back from the victim. Specifically, the host follows the same path (shortest path) across the routers for sending the packet to its destination. Make Over and Dump component maintains the information about each host and its equivalent packet marking value. If the marking value matches the stored value, it forwards the packet to respective host. During the time of the attack, when host spoofs the IP address of another host, the packet marking value differs from the value stored in the Make Over and Dump filter. This happens because: For marking, MATCH filter uses MAC address instead of the IP address. Therefore, the packets are dumped at the victim side and Make Over and Dump requests for the trace-back.

4.3 The Dıffıe- Hellman Key Exchange Algorithm Takes Place İn Following Steps [29]

1. Alice and Bob, using insecure communication, agree on a huge prime p and a generator g. They don't care if someone listens in.
2. Alice chooses some large random integer $x_A < p$ and keeps it secret. Likewise Bob chooses $x_B < p$ and keeps it secret. These are their "private keys".
3. Alice computes her "public key" $y_A \equiv g^{x}_{A} \pmod p$ and sends it to Bob using insecure communication. Bob computes his public key $y_B \equiv g^{x}_{B}$ and sends it to Alice. Here $0 < y_A < p$, $0 < y_B < p$. As already mentioned, sending these public keys with insecure communication is safe because it would be too hard for someone to compute x_A from y_A or x_B from y_B, just like the powers of 2 above.
4. Alice computes $z_A \equiv y_B{}^{x}{}_{A} \pmod p$ and Bob computes $z_B \equiv y_A{}^{x}{}_{B} \pmod p$. Here $z_A < p$, $z_B < p$. But $z_A = z_B$, since $z_A \equiv y_B{}^{x}{}_{A} \equiv (g^{x}{}_{B})^{x}{}_{A} = g^{(x}{}_{A}{}^{x}{}_{B)} \pmod p$ and similarly $z_B \equiv (g^{x}{}_{A})^{x}{}_{B} = g^{(x}{}_{A}{}^{x}{}_{B)} \pmod p$. So this value is their shared secret key.

V. CONCLUSION

HTTP or XML-Based DoS attacks are one of the most serious threats to cloud computing. Detection of these attacks can be effectively done by using marking approach based on packets on the attacker side and the detected packets are filtered by dropping the marked packets on the victim side. Therefore, the packet marking overhead and the false positive rate of DoS attacks are effectively reduced. DDoS attack detection scenario is improved by replacing the Cloud Protector with Make Over and Dump on the victim side and the introduction of MATCH filter and MARK filter at the source side. By this, enhancement of the reduction of the false positive rate is done and increase in the detection and filtering of DDoS attacks is possible. By the use of DIFFIE-HELLMAN KEY EXCHANGE algorithm, the victim can never be able to access the original text..

REFERENCES

[1] A.Belenky and N.Ansari (2003), 'Tracing Multiple Attackers with Deterministic Packet Marking (DPM)', Proceedings of IEEE Pacific Rim conference on communications, computers and signal processing, Vol. 1, pp. 49–52.

[2] A.Chonka W. Zhou and Y.Xiang (2008a), 'Protecting Web Services with Service Oriented Traceback Architecture', Proceedings of the IEEE eighth international conference on computer and information technology, pp. 706-711.

[3] A.Chonka, W.Zhou and Y.Xiang (2008b), 'Protecting Web Services from DDoS Attacks by SOTA', Proceedings of the IEEE fifth interna-tional conference on information technology and applications, pp. 1-6.

[4] A.Chonka, W.Zhou, J.Singh and Y.Xiang (2008c), 'Detecting and Tracing DDoS Attacks by Intelligent Decision Prototype', Proceedings of the IEEE International Conference on Pervasive Computing and Communications, pp. 578-583.

[5] A.Chonka, W.Zhou and Y.Xiang (2009a), 'Defending Grid Web services from X-DoS Attacks by SOTA', Proceedings of the third IEEE international workshop on web and pervasive security (WPS 2009), pp. 1-6.

[6] A.Chonka, W.Zhou and J.Singh (2009b), 'Chaos Theory Based Detec-tion against Network Mimicking DDoS Attacks', Journals of IEEE Communications Letters, Vol. 13, No. 9, pp. 717-719.

[7] A.Chonka, Y.Xiang, W.Zhou and A.Bonti (2011), 'Cloud Security Defence to Protect Cloud Computing against HTTP-DoS and XML-DoS attacks', Jour-nal of Network and Computer Applications, Vol. 34, No. 4, pp. 1097-1107.

[8] D.Dean (2002), 'An algebraic Approach to IP traceback', Journal ACM Transactions on Information and System Security', Vol. 5, No. 2, pp.119-137.

[9] S.Savage, D.Wetherall, A.Karlin and T.Anderson (2000), 'Practical Network Support for IP traceback', Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Com-puter Communication, pp. 295-306.

[10] H.Shabeeb, N.Jeyanthi and S.N.Iyengar (2012), 'A Study on Security Threats in Clouds', Journal of Cloud Computing and Services Sci-ence, Vol. 1, No. 3, pp. 84-88.

[11] X.Xiang, W.Zhou and M.Guo (2009), 'Flexible Deterministic Packet Marking: an IP Traceback System to Find The Real Source of At-tacks', Journal of IEEE Transactions on Parallel and Distributed Sys-tems, Vol. 20, No. 4, pp. 567-580.

[12] K.H.Choi and H.K.Dai (2004), 'A Marking Scheme using Huffman Codes for IP Traceback', Proceeding of 7th International Symposium on Parallel Architectures, Algorithms and Networks (SPAN'04).

[13] E.Anitha and Dr.S.Malliga (2014), 'A Packet Marking Approach To Protect Cloud Environment Against DDoS' Computer Science and Engineering Department, Kongu Engineering College Perundurai, India mallisenthil@kongu.ac.in.

[14] A.Parvathi and G.L.N.JayaPradha (2011), 'An IP Trace back System to Find the Real Source of Attacks', International Journal of Computer Trends and Technology- volume 2 Issue 1.

[15] K.Santhi, (2013), 'A Defense Mechanism to Protect Cloud Computing Against Distributed Denail of Service Attacks, volume 2, Issue 5, May 2013.

[16] Nisha H. bhandari (2013), 'Survey on DDoS Attacks and its Detection & Defence Approaches' IJISME.

[17] R. Vivek, R. Vignesh & V. Hema (2013), 'An Innovative Approach to Provide Security in Cloud by Prevention of XML and HTTP DDoS Attacks' ISSN(PRINT : 2320-8945, volume-1,Issue-1,2013.

[18] John Ioannidis, Steven M. Bellovin (2010) 'Implementing Pushback: Router-Based Defense Against DDoS Attacks' .

[19] J.J. Shah, Dr. L.G. Malik (2013), 'Impact of DDOS Attacks on Cloud Environment', Communication Technology, vol 2, Issue 7, July-2013.

[20] Amit Vinayakrao, Narendra Shekokar, Mahesh Maurya (2014) 'The Countering the XDoS Attack for Securing the Web Services', (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,3907-3911.

[21] Neha Tirthani, Ganesan R, 'Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography', School of computing Sciences and Engineering, M. tech–Computer Science, Associate Professor (CSE), VIT, Chennai campus.

[22] A.J.Han Vinck, University of Duisburg-Essen SVG version: Flugaal ,'Introduction to public key cryptography', p. 16.

[23] Merkle, Ralph C (April 1978). "Secure Communications Over Insecure Channels". Communications of the ACM 21 (4): 294–299. doi :10.1145/359460.359473. Received August, 1975; revised September 1977.

[24] Diffie, W. ; Hellman, M. (1976). " New directions in cryptography" (PDF). IEEE Transactions on Information Theory 22 (6): 644–654. doi :10.1109/TIT.1976.1055638.

[25] Ellis, J. H. (January 1970). "The possibility of Non-Secret digital encryption".

[26] Martin E. Hellman, Bailey W. Diffie, and Ralph C. Merkle, "Cryptographic apparatus and method", issued 29 April 1980.

[27] A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic," Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé, Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science, Volume 8441, 2014, pp 1-16.

[28] C. Kaufman (Microsoft) (December 2005). "RFC 4306 Internet Key Exchange (IKEv2) Protocol". Internet Engineering Task Force (IETF).

[29] http://www.google.com .