Security Solutions for Cloud Computing

Aarti Potdar
Dept. of Computer Engineering
MIT College of Engineering, Pune

Pranav Patil
Dept. of Computer Engineering
MIT College of Engineering, Pune

Raunak Bagla
Dept. of Computer Engineering
MIT College of Engineering, Pune

Rohitashwa Pandey
Dept. of Computer Engineering
MITCollegeof Engineering,Pune

ABSTRACT
In the recent times, most organizations in the world have increasingly realized the importance of cloud platforms. Cloud computing is an emerging technology to store and access personal data along with business information from remote locations. One of the benefits of using cloud computing is the ability to tap into huge quantities of both structured and unstructured data. With every new technology there are certain drawbacks associated with it and cloud is no exception. Unlike others, Cloud environment also faces challenges such as Distributed denial of service (DDoS) attacks, data thefts, particularly when they are insider attacks. Increase in the number of DDoS attacks is one of the latest issues. We have studied various intrusion detection techniques that includes Cloud trace back model, use of back propagation neural network and Virtual Intrusion Detection Systems (V-IDS). Now these attacks can be prevented using the proposed Intrusion Prevention System i.e. Service-based Intrusion Prevention System in Cloud Computing (SIPSCC). A technique called fog computing can be used to detect and prevent data theft attacks by malicious insiders is studied.

General Terms
Cloud Computing Security

Keywords
Cloud Computing, Denial of Service, Intrusion prevention, Cloud Trace back Model, Intrusion Detection, Intrusion Prevention System, Fog Computing.

1. INTRODUCTION
Cloud computing is often simply referred as "the cloud". It delivers the on-demand computing resources over the Internet. Cloud computing involves deploying groups of software networks and remote servers that provides centralized data storage and online access to on-demand services or resources [8].There are three types of models in cloud computing: Public, Private and Hybrid.

Major purposes of cloud computing include Testing and Development, Big Data analytics, File Storage, Customer Relationship Management (CRM), reduction of costs and last but not least Universal access.Commonly used cloud services are Software as a service, Platform as a service and Infrastructure as a service. Software as a service can be accessed by distant computers, these machines can be owned and operated by different companies that can connect users via internet and web browser [5]. Platform as a service is a cloud-based environment which provides everything required for building a web-based application without the cost and complexities of buying and managing the hardware, software, provisioning and hosting the applications. [5]. Infrastructure as a service provides clients with computing resources including networking, servers, storage, data center space and onapay-per-usebasis [5]

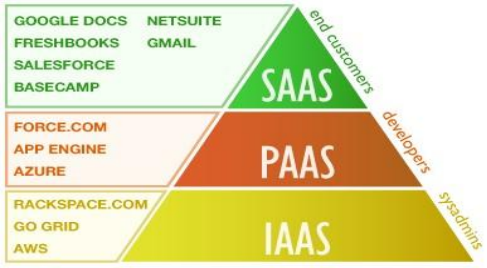

Figure 1: Cloud Services

The cloud service models have vastly developed resulting in delivering business-supporting technology more efficiently than ever before. Shifting from server to service-based thinking has transformed the way technology departments think about the designing and delivering the applications in computing technology. These advances in cloud computing have opened doors for new security issues whose full impact is still unknown. Major threats to cloud security are Data Breaches, Data loss, poorly developed Interfaces and APIs, Denial of Service, Malicious Insiders, Abuse of Cloud Services, Insufficient Due Diligence and Shared Technology Issues.

In this survey we will discuss the Cloud Trace back model for Intrusion Detection System, Network Intrusion prevention System, Cloud Trace back mark and Cloud Protection against DDOS attacks in FOG computation to prevent data breaches.

2. LITERATURE SURVEY
Cloud technology faces various issues in the field of security. The various types of attacks on cloud infrastructure include Data theft, DDOS, SQL injection, cross VM side channel, phishing botnets, etc. DDOS and SQL injection are widely used as shown in Fig 2.

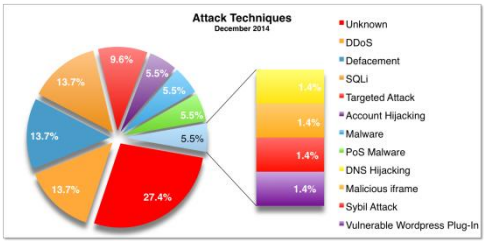

Figure 2: Cloud Attack statistics for Dec 2014 [10]

Studies by IBM shows that companies are attacked at an average of 16,856 times a year, and that many number of attacks result in a quantifiable data breach. These attacks

can cause a major setback in company's progress and hamper their reputation in global market as shown in Fig 3.

Figure 3: Consequences of cloud attacks on companies [9]

DDOS stands for Distributed Denial of Service. It is a type of attack which aims to make resources or services unavailable by flooding a victim with useless traffic. It results in temporarily or indefinite interruption of services on the host system. Attacker hides its identity from victim by spoofing its IP address [11].

SQL injection is a code injection technique used to attack data-driven applications in which malicious SQL statements are inserted into an entry field for execution.

3. EXISTING PROPOSED MODEL

The above mentioned attacks could be prevented using the following models.

3.1 Virtual Intrusion Detection System

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability issues against a target application or computer. An IDS only detects the threats in an out-of-band network infrastructure. IDS is a listen-only device i.e. it listens to the ongoing traffic. The IDS monitors traffic and reports its results to the administrator of the IDS, but is unauthorized to take any action to prevent a detected exploit from taking out of the system [1].

The proposed architecture should provide a set of functionalities which permits the reconfiguration of the cloud infrastructure to improve security.

The V-IDS architecture includes modules for monitoring, analysis, decisions, actions, and management as given in the.

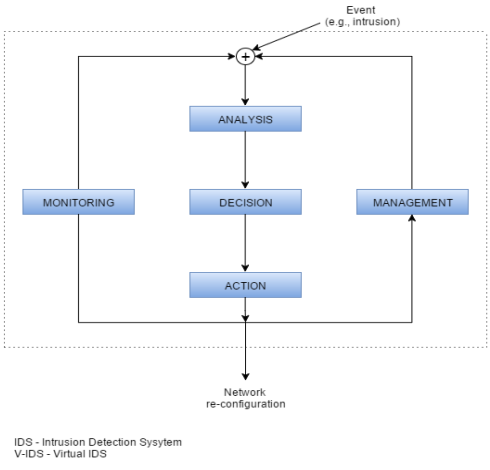

Figure 4: Conceptual IDS model [1]

Analysis module captures events coming from the network and provides an overall picture of the incoming traffic which enables the decision module to make decisions around automatic and adaptive adjustment and associated actionable responses [1].

Decision module is part of the closed chain control system that uses the data received from the analysis module and makes decisions on the real time actions necessary to solve anomalies related to network intrusions.Action module represents the actuator that solves the intrusion detection situation on a cloud domain. The V-IDS uses the results from the analysis in order to manage the cloud infrastructure on the basis of security. It also generates alarms, reports and queries if the analysis indicates a dangerous condition.

Monitoring module continuously captures processed data from previous events such as historical intrusion data, login attempts, and so on. Each event is time-stamped and stored in a sequential file sorted by time. The raw data captured by the monitoring module assists the analysis module in building a complete event correlation map suitable for decision adjustment and actionable response calculation.

Management module permits configuration and tuning of the V-IDS connected to the cloud infrastructure. A virtual IDS must be configured, updated and actively managed differently than a conventional IDS. An IDS with a poor management module will require excessive work and might even be useless if the required management work is poorly supported.

3.2 Service-based Intrusion Prevention System in Cloud Computing (SIPSCC)

An Intrusion Prevention System (IPS) holds all capabilities of IDSs, plus prevention characteristics. If an intrusion is detected by the mechanism a firewall rule can be applied, a routing configuration can be changed or a virtual machine can be isolated among security procedures.

Service-based Intrusion Prevention System in Cloud Computing (SIPSCC) is Intrusion Prevention System model defined to reduce intrusions. SIPSCC service works on three local modules through Open Source Host-based Intrusion Detection System (OSSEC) application, client and server [2]. The way in which the client server model works is shown in Fig 5, the client will receive the configuration from the server and then client sends the logs to the server through an encrypted channel by UPD port [2].

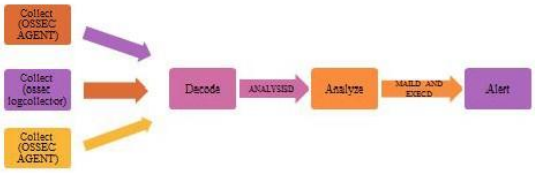

Figure 5: Working of SIPSCC [2]

The artifact is worked on a local mode as shown in Fig 6 and this method means that all logs will be sent to the server from network systems. Generic log analysis of the breakdown is as below. The log collecting is done through a log collector, then decoding and analysis are completed by analysis. Next the alerting goes through by mail-lD and finally the active responses are from analysis [2].

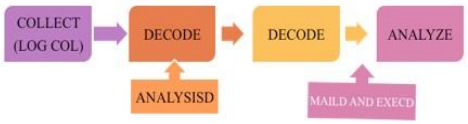

Figure 6: Local model of SIPSCC [2]

Sqlmap is Intrusion Prevention System software based on SIPSCC model which will be discussed in results.

3.3 Cloud Trace Back Model

Cloud Trace Back Model (CTB) proposed here provides solution to trace back to find the host of the attack. The application module proposed here helps to trace back DDOS attacks, in return determining the source of the attack. Main objective of CTB is to apply Service Oriented Approach (SOA) in Trace back methods. It is a design pattern, a formal way of documenting a solution to a design problem. CTB is based on Deterministic Packet Marking (DPM). Here reserved flag and ID field are marked in the IP header. Incoming packets are marked when they enter ingress router on the server, the outgoing packets are ignored usually. The marked packets remain unchanged throughout the network [3].

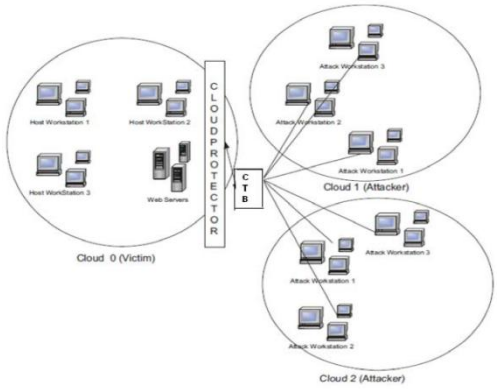

Figure 7: Proposed Model

3.4 Proposed Model

Here it has been proposed that in a CTB framework, FDMP methodology is to be employed. It is done by placing their Cloud Trace back Mark (CTMB) within the web service. It is to be deployed at edge routers of source end. System becomes vulnerable to attacks if there are no security services present on the network. CTB is placed just before the web servers and CTBM is placed within the CTB header. All service requests are marked first, hence it removes service provider's address preventing any direct attacks. If an attack occurs the victim can recover the CTM tag which can immediately reveal the identity of host [3].

3.4.1 Process flow: Attack Scenario

1. Attack client requests webserver through CTB.
2. SOAP request message is formulated by client based on the service description requirements and the request is sent to CTB.
3. CTB marks it with CTM within header and forwards the request to the web server.
4. If an attack is detected by the system, reconstruction is requested.
5. The system Extracts the mark and informs the administrator or the user on the origin location of the attack.
6. Simultaneously the attack traffic can be filtered out.

A Cloud Protector model has been proposed as well which overcomes CTB which does not prevent DDOS attacks. Cloud Protector acts in filter section of the Defense System. It is a trained back propagation neural network (NN), it detects and filters out DDOS messages. Neural network is made up of set of layers: Input, Output and Hidden layer. Threshold logic unit (TLU) is focused in case of NN. Each layer in the NN has a weight associated with it, it inserts input object in an array of weighted quantities. Then sums up the traffic to check whether it crosses threshold limit. If any suspicious activity is detected, the Cloud Protector blocks the suspected traffic [3].

3.5 FOG COMPUTING

Implementation of cloud includes placing data in the hands of a third party, thus it must be ensure the data security when the data is at rest as well as when it is in transit. Data security is of paramount importance in any case. Data resting in the cloud needs to be accessible only by authorized personnel. In order to ensure the integrity of user authentication, cloud providers need to access the data access logs and verify that only authorized users are accessing the data. These access logs also need to be securely maintained. There are some traditional security mechanisms like identity, authentication and authorization but now these are not sufficient [5].

Here they have used a different approach for securing the data in the cloud by using decoy information technology. This technology is appropriately called fog computing as its basic purpose is to reduce the visibility of the information to the attacker. On recognition of an un-authorized access to the account, disinformation attacks are launched against malicious insiders, preventing them from getting access to user real data. Many accidents happen which damage the data or the data can be stolen and information once lost cannot be retrieved again. Thus the basic idea of fog computing is limiting the damage of stolen data by reducing the value of the data Securing Cloud Computing Using FOG Computing. This is achieved by using preventive disinformation attack [4].

3.5.1 User behavior profiling

User behavior profiling is a technique that is applied to monitor how, when and how much a user accesses information in the cloud account [4]. This is known to be the normal behavior of the user. This behavior is continuously monitored and verified to check whether any abnormal behavior or a suspicious activity has occurred. If an abnormal behavior is detected, it is suspected that the account has been breached and any further data access is unauthorized access. This method of security is mainly used in fraud detection systems.

3.5.2 Decoys

A decoy is a person or a device or an event used for distracting, concealing the true information of the secure data by replacing it by Decoy information, bogus records, honeypots or various honey files to distract the attacker. Decoys are used to poison the stolen data. Decoys confuse

the attack and make them believe that they have ex-filtered useful information when actually they have not. This technology along with User Behavior Profiling can be used to efficiently secure the data in the cloud.

3.5.3 Masquerade Detection

In the paper, these concepts have been applied to detect illegitimate data access by masqueraders or the attackers who impersonate legitimate users after stealing their identity. Following experimental results that were achieved by using this approach in detection of masquerade activity in local file setting. If we combine User Behavior Profiling and Decoy Technology for Masquerade Detection, the threats can be detected from a search pattern. If a legitimate user searches for a particular file or a document, the search criterion will be specific and targeted. On the contrary a masquerader or an outsider with limited access to the administrator account is not likely to be familiar with the structure of the file system, thus the search criterion of such masquerader will be non-targeted and widespread.

The previous experiments have validated the assumption and demonstrated that masquerade attacks can be reliably detected and prevented with a very low false positive rate of 1.12% [6]. Monitoring and detecting abnormal searches, adding decoy traps combined together may make a very efficient masquerade detection system. Combining the two techniques effectively improves detection accuracy. To conduct this review, eighteen classifiers were trained with computer usage data and the usage data of the 18 computers was collected over a period of 4 days. Eighteen classifiers were created using the search behavior anomaly detection as described in their previous paper [5] and another 18 classifiers were created using a detection approach that combined user behavior profiling along with access local system placed decoy files. These classifiers were then tested using simulated masquerader data.

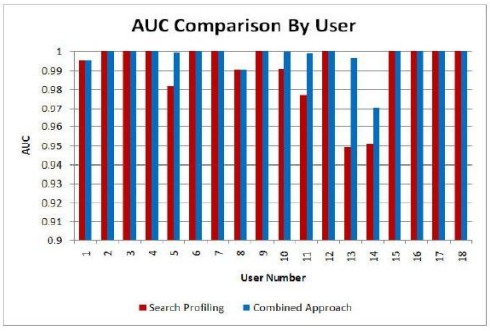

Figure 8: Comparison by User Model for Search Profiling and Integrated Approaches [4]

The results of the test performed showed that the models using the combined detection approach achieved equal or better results than that of the search profiling approach alone. Using this approach, they were able to improve the accuracy of the detector. Combining the two techniques may lower the overall false positive rate of detector.

4. RESULTS OF PROPOSED MODELS

The Author created a website with a total of 21 vulnerabilities and evaluated the vulnerabilities detected, average time, and false positives in the website using Sqlmap software based on SIPSCC model. The author evaluated the parameters of WebCruiser, Netsparker, Acunetix, and NVSs vulnerability and detected 15/21, 16/21, 18/21 and 21/21 in average time per hour 0.15, 1.2, 2.24, and 0.01. The False Positive in this sequence was 1, 3, 12, and 0 [12]. Author's evaluation resulted in the parameter of Sqlmap vulnerability and detected 19/21 vulnerable in 0.25 average times per hour with a False Positive of 4.

Evaluation by Singh and Roy (2012)					Authors Tools
Parameter	Web-Cruiser	Netsparker	Acunetix	NVS	Aqlmap
Vulnerability	15 of 21	16 of 21	18 of 21	21 of 21	19 of 21
Average Time (hr)	0.15	1.2	2.24	0.01	0.25
False Positive	1	3	12	0	4

Figure 9: Evaluation [12]

Cloud Trace back Model was able to detect 76-81 % of attack traffic as shown in fig 10. Thereby, it can be concluded that CTB has an accuracy of around 75%.The previous experiments on proposed fog computing have validated the assumption and demonstrated that masquerade attacks can be reliably detected and prevented with a very low false positive rate of 1.12% [6].

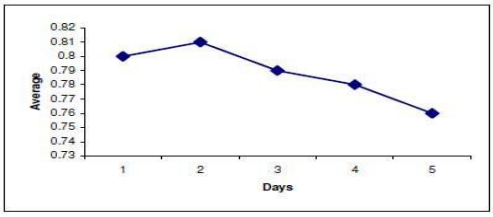

Figure 10: Avg. attack traffic detected by CTB

5. CONCLUSION

In conclusion, all the proposed models have been proved by the authors to be performing on a competent level. But, In order to reduce the number of attacks, the cloud security models proposed above cannot be used together. It is not feasible to implement all models on a single cloud infrastructure as it will add unsupportable overhead on the hardware as well as software. Thus an improved security system which incorporates the functionalities of all the models discussed above is required. Such a security system should provide maximum security while being light on the cloud infrastructure.

6. REFERENCES

[1] Pasquale Donadio, "Virtual Intrusion Detection Systems in the Cloud", Bell Labs Technical Journal 17(3), 2012, pp 113-128

[2] Saeed M. Alqahtani , Maqbool Al Balushi, Robert John, "An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC)" in 2014 International Conference on Computational Science and Computational Intelligence, IEEE, 2014, pp 152-158

[3] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar

[4] Joshi, "Securing Cloud Computing Environment Against DDoS Attacks" DOI:10.1109/ICCCI.2012.6158817

[5] Salvatore J. Stolfo, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud",2012, Under license to IEEE.DOI 10.1109/SPW.2012.19

[6] Marinos A. and Briscoe G., "Community Cloud Computing", (pp. 472-484). Heidelberg: Springer, 2009, pp. 472- 484

[7] M. Ben-Salem and S. J. Stolfo, "Modeling user search behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 120.

[8] "Cloud Computing Vulnerability Incidents: A Statistical Overview", Cloud Security Alliance, August 23, 2012; Revised March 13, 2013

[9] http://www.ibm.com/cloud-computing/

[10] www.ibm.com/services/us/en/it-services/securityservices/data-breach/

[11] https://paulsparrows.files.wordpress.com/2015/01/

[12] Trostle J, (2006), protecting Against Distributed Denial of service attacks Using Distributed Filtering, Securecomm and Workshops, Aug 28 2006- sept1 2006, pp 1-11

[13] A. K. Singh and S. Roy, "A network based vulnerability scanner for detecting sqli attacks in web applications" in Recent Advances in Information Technology (RAIT), 2012 1st International Conference on. IEEE, 2012, pp. 58.