International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

# COMPARISON OF INTRUSION DETECTION TECHNIQUES IN CLOUD COMPUTING

**Mr K. Srinivas Babu[1], Dr K. Rameshwaraiah[2]**
[1]*Research Scholar S V University, Tirupathi*
[2]*Professor and Head NNRESGI, Hyderabad*

**Abstract—** Cloud computing is a kind of computing, which is highly scalable and use virtualized resources that can be shared by the users. Cloud computing provides scalable services to end users with greater flexibility and less infrastructure. Cloud services include software as a service, platform as a service, and infrastructure as a service. These services are provided by using different protocols and standards. Economic benefits are the main driver for the cloud, since it promises the reduction of capital expenditure and operational expenditure. One of the most significant search done on cloud computing is to provide security to the cloud environment. Cloud computing can be threatened by various cyber attacks, because most of the cloud computing systems provide services to many people who are not proven as trustworthy. In this paper, we are going to compare the techniques to detect the intrusion in cloud computing. The techniques used are Signature Based detection (SD), Anomaly-based Detection (AD) and Stateful Protocol Analysis.
**Keywords—** *Anomaly based, Bayesian model, Decision trees, Signature-based, Stateful protocol.*

## I. INTRODUCTION

Before emerging the cloud computing, there exists a client/server computing which is a central storage for all software applications, data and controls are residing on the server side, then distributed computing came into existence [1]. Cloud services are as cheap and convenient for hackers as are for service customers [2]. In 1961, John Macharty introduced cloud computing. The aim of Cloud computing is to provide on-demand network access to shared resources. It provides scalable services to end users with high flexibility and less investment. Cloud computing provides better utilization of resources using utilization techniques a fight with security risks. It increases the capacity or add capabilities without changing the infrastructure [3].

Cloud service providers offer guarantees in the terms of service availability and performance during a time period of hours and days.Cloud provider must pay a penalty if the cloud requirements are not satisfied [4]. The cloud provides instant global platforms, elimination of H/S capacities and licenses reduced cost, simplified scalability. Adopting cloud network redundancy disaster recovery risks and high costs [5].

The above figure 1 depicts the cloud computing. Cloud computing is a model for enabling convenient, on demand network access to shared computing resources (ex: network, servers, storage, applications and services). Cloud computing has become a social phenomenon used by most people every day [6].

 

*Fig. 1. Cloud Computing (Source: Internet of Things: A Transformational Force for the Insurance Industry, 2015)*

## II. CLOUD SERVICES

There are three main cloud services in cloud computing. They are:

1. Software as a Service (SaaS): Cloud consumers release their applications in a hosting environment which can be accessed through networks from various clients by application users [6].
Web browsers are commonly used to provide access to SaaS application. An example of SaaS is Google Mail [7].

2. Platform as a Service (PaaS): This is a platform where it supports "Software Lifecycle"which allows the cloud consumers to develop cloud services and applications directly on the PaaS cloud [6].
Web services and Web browsers are used to provide access to PaaS applications. An example of PaaS is Google AppEngine [7]. It includes all of the API's for a specific programming language of a server [8].

3. Infrastructure as a service (IaaS): Here the cloud consumers use IT infrastructure provided in an IaaS cloud [6].
Web services are commonly used to provide access to SaaS application. An example of IaaS is Amazon's EC2 [7].
Users have access only to the virtualized infrastructure layer through the virtual machine abstraction of different hardware components [8].

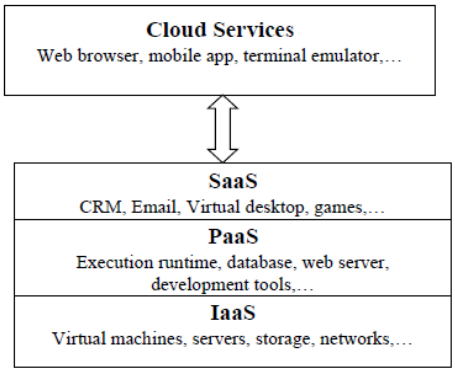


*Fig. 2. Cloud Services*

The above figure 2 demonstrates the services of cloud. All the three categories of the cloud services are described in detail above the diagram.
The use of cloud computing is becoming popular due to its mobility, low cost and huge availability [9]. Consumers can use the services wherever internet access is possible, therefore it is an excellent aspect of accessibility [10]

 

## III. CLOUD ARCHITECTURE

The cloud computing reference architecture identifies the major actors, their activities and functions in cloud computing and it is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing. The cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker [11].

**A. Cloud Consumer:** The cloud consumer is the principal stakeholder in the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider and uses the service. The cloud consumer may be billed for the service provisioned and needs to arrange payments accordingly.

**B. Cloud Provider:** A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties. A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

For SaaS, the cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure.

For PaaS, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components.

For IaaS, the Cloud Provider acquires the physical computing resources underlying the service, including the servers, networks, storage and hosting infrastructure.

**C. Cloud Auditor:** A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system.

**D. Cloud Broker:** As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

In general, a cloud broker can provide services in three categories: Service Intermediation, Service Aggregation, Service Arbitrage.

 

**E. Cloud Carrier:** A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication and other access devices. A cloud provider will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

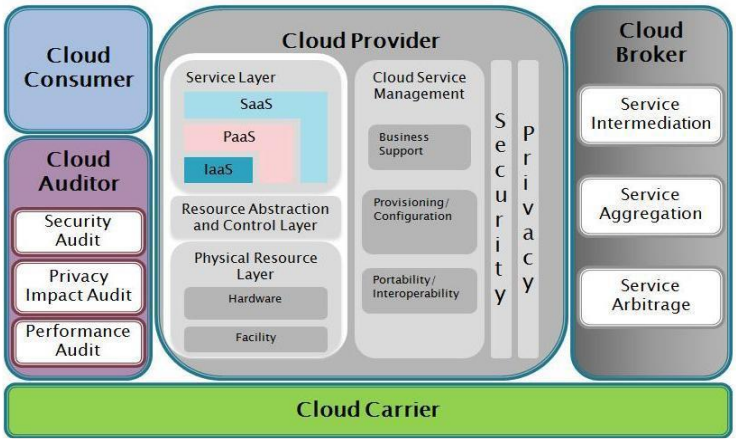


***Fig. 3. Cloud Reference Architecture (Source: NIST Cloud Computing Reference Architecture, 2013)***

The above figure 3 depicts the architecture of the cloud computing architecture.

## IV. CHARACTERISTICS OF CLOUD COMPUTING

Following are the characteristics of the cloud computing are [12].

1. **Elasticity:** It is a core feature of cloud systems which confines the underlying infrastructure capability to adapt to changing requirements such as the amount and size of data used in an application.

2. **Reliability:** It is the capability of ensuring the continuity of the system operation without disruption such as loss of data or code reset during execution.

3. **Quality of Service:** This feature is important for specific requirements which should be met through the provided services or resources.

4. **Agility and Adaptability:** These are the two key features of great concern to cloud systems relevant to the elastic capabilities. Agility and adaptability require management of the resources to be autonomous.

5. **Availability:** This is the ability of providing redundant services and data to mask failures transparently. With the increase of access, availability is attained through replication of services or data and disseminating them across various resources.

## V. DEPLOYMENT OF CLOUD SERVICES

Cloud services can be deployed in four ways depending upon customer's requirements [13]:

A. **Public Cloud:** A cloud infrastructure is provided to many customers and is managed by a third party.

 

B. **Private Cloud**: A cloud infrastructure made available only to a specific customer and managed either by the organization itself.
C. **Community Cloud:** Infrastructure shared by several organizations for a shared cause and may be managed by them.
D. **Hybrid Cloud:** A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other.

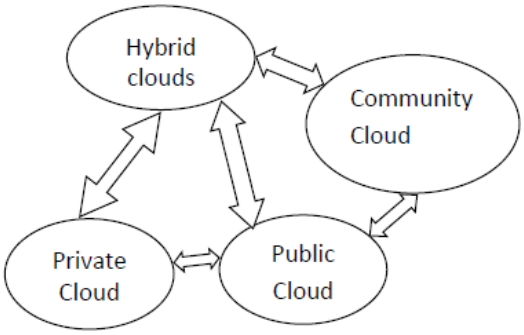


***Fig. 4. Deployment of Cloud Services***

The above figure 4 illustrates the deployment of cloud services.

## VI. LITERATURE SURVEY

To manage some internal resource frameworks and few techniques are introduced like verification framework for hybrid clouds, hash index hierarchy, homomorphism.

There are non-conventional techniques for securing the cloud network from malicious insiders and outsiders, i.e., research gap identifiers, Anomaly detection stage, Prototype implementations. To protect the cloud from cyber attacks service oriented paradigms, multi-domains, on-demand elasticity are used. Service Level Agreement improves the quality of service being delivered in the cloud. Masquerade attack is one where an attacker assumes the detect this we need to move the data to different environments to increase its usability and keep safe from attackers [14].

Security and reliability are two important factors that companies, mostly concern after shifting business processes onto cloud Computing [15]. For anomaly detection in cloud computing Bayesian classifiers & decision trees have been implemented.

1. **Decision Tree**: A decision tree is a hierarchical model with local regions identified in a sequence of recursive splits.

It is composed of internal decision nodes and terminal leaves. Each decision node n implements a test function fn(d)with discrete outcomes.

When a test hits a leaf node, the classification labeled on the leaf is output.

For a node n in the decision tree, the entropy is calculated by,

$$H(n)= -\sum_{i=1}^{j} pin \log_2 pin \qquad (1)$$

where: j=number of classes
pin=probability of the class
Decision Trees have such disadvantages as:

 

Most of the algorithms require that the target attribute will have only discrete values.
As the decision trees use the 'divide and conquer' method, they tend to perform well if a few highly relevant attributes exist, but less so if many complex interactions are present.

2. **Bayesian Classifier**: This classifier is used to predict the probability of a given network that belongs to a particular class.

It has the highest accuracy and speed than the others classifiers [16].

Let us consider X a given packet. H is a hypothesis that belong to a class C. We need to determine the probability P(H|X).using Bayes theorem the probability of P(H|X) is given by,

$$P(H|X)=P(X/H)P(H)/P(X) \quad (2)$$

Where: P= probability of the class
X= given packet
H= hypothesis that belongs to class C

The advantages of Bayes classifier are:
It uses a very spontaneous technique, i.e., they do not have several free parameters that must be set.
It does require any large amount of data before learning can be begin.
Bayes Classifiers are computationally fast when making decisions.

## VII. MAJOR CHALLENGES/ISSUES

Security is the greatest issue that is caused in cloud computing, which reduces the growth of it and privacy, data protection . Some of the security challenges are data storage security, application security & data transmission security [17]. Due to the lack of control on security users of cloud are using less sensitive data. Cloud computing involves three parties; cloud customer, cloud service provider and cloud network. These are the security threats which cause damage to the cloud [18]. Some of them are:

1. Guest hopping attack: Separation failure between shared infrastructures.
2. SQL injection: Attack websites.
3. Site channel attack: Attacker places some malicious virtual machine on the same physical machine as the victim machine
4. Data storage security: Users data are stored in the cloud service provider which runs simultaneously, which may be harmed by the attackers.

As the cloud consumers do not have the control over the computing resources they have to ensure the quality, availability, reliability and performance of the reuse. Cyber attacks represent a serious danger which can decrease the quality of service which has to be delivered to the consumers.

In a shared tendency cloud computing environment, data can be run on different virtual machines, but is stored in a single physical machine which provides flexibility, but attackers can easily attack or duplicate data on a single machine. It is also easy to perform brute-force attacks on the passwords that have kept for data, it does not take long time for them to open the resources [19].

The next cyber security threats can be targeted on specific government agencies and organizations or individuals within enterprises and including cloud serving providers. It could be easy to reveal the

 

information by a third party rather than insiders [20]. Some important data and applications are held by a third party they are not understood and complex, due to which there is a lack of control and transparency. Cloud customer has no idea about the exact location of the data as there are privacy restrictions [21].

The cloud holds the customers' data in a shared place where the data is not stored sequentially. The failures and the disasters that are caused in cloud cannot be recovered. Intruder attempts are hard to track as the resources are shared in the cloud. There is no guarantee of the data that is available always resides in the cloud. It is challenging to justify the cost of the resources in case of cloud services. Customers need to think of different methods regarding the cost of security, communication, integration and computing power.

## VIII. INTRUSION DETECTION TECHNIQUES

There are some techniques to detect the intrusion that occurs in the cloud computing environment. They are:

1. Signature-based Detection: A set of rules that can be used to design given pattern is that of an intruder.
2. Anomaly-based Detection: Identifying events that appear to be anomalous with respect to normal system.
3. Stateful Protocol Analysis: the intrusion detection system could know and trace the protocol states.

### A. **Signature-based Detection**

A signature is a pattern that approaches a threat. Signature based Detection is the process to compare patterns against captured events for recognizing possible intrusions. It is also called as Knowledge-based or Misuse-based Detection. The signature based detection system is capable of attaining a high level of accuracy and less false positives in identifying intrusions. This is an efficient solution for detecting known attacks but fails to detect unknown attacks. It is used in either front end of the cloud to detect external intrusions or at the back end to detect the internal/external intrusions. The analysis of events involves signature-based methods. Features extracted from logged event data are compared to features in attack signatures which in turn are provided by experts [22].

### B. **Anomaly-based Detection**

Anomaly detection is concerned with identifying events that appear to be anomalous with respect to normal system behaviour. The anomaly based approach involves the collection of data relating to the behaviour of legitimate users over a period of time, and then apply statistical tests to the observed behaviour, which determines whether that behaviour is legitimate or not [23]. .In this technique, it detects known, as well as unknown attacks. Anomaly detection techniques are used to detect unknown attacks at different levels.

### C. **Stateful Protocol Analysis**

Stateful protocol analysis provides capabilities for understanding and responding to attacks. It is also known as deep packet inspection. It can identify unexpected sequences of command such as same command issued repeatedly or not issuing the command where it has to be dependent.

It can also detect variations in command length, minimum and maximum values of attributes and potential anomalies. The biggest limitation of stateful protocol inspection for intrusion detection is the resource requirements are not sufficient.
Some of the other intrusion detection approaches are [24]:

 

1. **Artificial Neural Network**: It is used to generalize data from incomplete data and able to classify whether it is normal or intrusive. This is not an efficient solution to detect intrusions for cloud as it requires a quick intrusion detection mechanism.

2. **Association Rule Based**: In this approach, the signature based algorithm generates a signature for misuse detection. Scanning reduction algorithm was introduced to reduce the number of databases for generating signatures or attacks from previously known.

3. **Support Vector Machine Based**: This approach is used to detect intrusions based on limited sample data. This approach is better than the artificial neural network as it produces less false positive rates.

4. **Genetic Algorithm based**: This approach is used to select network features that can be used in Entropy=quantify impurity other techniques for achieving results optimization. Some rules are introduced to detect the new intrusions in the cloud. These rules are generated from network features.

5. **Hybrid Techniques**: These are the techniques that are formed when the above two or more techniques are combined. This is advantageous among all the techniques.

## IX. COMPARISION BETWEEN SIGNATURE-BASED, ANOMALY-BASED AND STATEFUL PROTOCOL ANALYSIS DETECTION

The above table 1 shows the comparison between signature-based, anomaly based and stateful protocol detection. From the above comparison, we can say that anomaly based detection is the best method to find out the intrusions occurred in cloud computing.

***Table. 1. Comparision of intrusion techniques***

| IDS/IPS Technique | Characteristics | Challenges |
|---|---|---|
| Signature-based Detection | 1. Identifies intrusion by matching captured patterns with preconfigured knowledge base.<br>2.High detectsion accuracy of previously known attacks.<br>3.Low computational cost | 1. Cannot detect new known attacks.<br>2.Knowledge base of matching should be crafted carefully.<br>3. High false alarm rates for unknown attacks. |
| Anomaly Detection | 1. Uses statistical tests to identify intrusion.<br>2.Can lower the false alarm for unknown attacks. | 1. The more time required to identify the attacks.<br>2. Detection of accuracy is based on amount of collecting behaviour. |
| Stateful Protocol | 1. Identifies unexpected sequences of command.<br>2. Add stateful characteristics to regular protocol analysis.<br>3. Reasonable checks thresholds for individual commands. | 1.Lots of overhead<br>2. Cannot detect the attacks that do not violate the characteristics of the protocol.<br>3. Conflicts between the protocol model used by IDPS. |

## X. CONCLUSION

As described in the paper, though there are advantages in using cloud environment, there are some practical problems that must be solved. Quality, reliability must be ensured proper. In the above paper, the issues in cloud computing can be solved by using the anomaly detection methods, i.e. Bayesian Classifiers and Decision Tree. Secondly stateful protocol is used to detect the issues in cloud computing. Signature-based detection is used in the worst case.

## REFERENCES

[1] Ficco, M., Tasquier, L., & Aversa, R. (2013, October).“Intrusion detection in cloud computing”. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on (pp. 276-283). IEEE

[2] Patel, A., Taghavi, M., Bakhtiyari, K., &JúNior, J. C. (2013).“An intrusion detection and prevention system in cloud computing: A systematic review.” Journal of network and computer applications, 36(1), 25-41.

[3] Gupta, S.,Kumar, P.,Abraham, A. (2013).“A profile based ntwork intrusion detection and prevention system for securing cloud environment”. International Journal of Distributed Sensor Networks, 2013

 

[4] Ficco, M., Venticinque, S., & Di Martino, B. (2012, September).“Mosaic-based intrusion detection framework for cloud computing”. InOTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 628-644). Springer Berlin Heidelberg.
[5] Ercan, T. (2010).”Effective use of cloud computing in educational institutions”. Procedia-Social and Behavioral Sciences, 2(2), 938-942.
[6] Dillon, T., Wu, C., & Chang, E. (2010, April).”Cloud computing: issues and challenges”.In 2010 24th IEEE international conference on advanced information networking and applications (pp. 27-33).Ieee.
[7] Jensen, M., Schwenk, J., Gruschka, N., &Iacono, L. L. (2009, September).“On technical security issues in cloud computing”. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). IEEE
[8] Zargar, S. T., Takabi, H., & Joshi, J. B. (2011, October).” DCDIDP: A distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments”. InCollaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on (pp. 332-341). IEEE.
[9] Petre, R. S. (2012).”Data mining in cloud computing. Database Systems Journal”, 3(3), 67-71.
[10] Lee, J. H., Park, M. W., Eom, J. H., & Chung, T. M. (2011, February).“Multi-level intrusion detection system and log management in cloud computing”. In Advanced Communication Technology (ICACT), 2011 13th International Conference on (pp. 552-555). IEEE
[11] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500(2011), 292.
[12] Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications, 36(1), 25-41.
[13] Hadauria, R., Chaki, R., Chaki, N., &Sanyal, S. (2011).”A survey on security issues in cloud computing”.IEEE Communications Surveys and Tutorials, 1-15
[14] Kholidy, H. A., &Baiardi, F. (2012, April).“CIDD: a cloud intrusion detection dataset for cloud computing and Masquerade attacks”. In Information Technology: New Generations (ITNG), 2012 Ninth International Conference on (pp. 397-402). IEEE.
[15] Huang, T., Zhu, Y., Zhang, Q., Zhu, Y., Wang, D., Qiu, M., & Liu, L. (2013, July).”Anlof-based adaptive anomaly detection scheme for cloud computing”. In Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual (pp. 206-211). IEEE.
[16] Guan, Q., Zhang, Z., & Fu, S. (2012). “Ensemble of bayesian predictors and decision trees for proactive failure management in cloud computing systems”. Journal of Communications, 7(1), 52-61.
[17] Claycomb, W. R., &Nicoll, A. (2012, July).“Insider threats to cloud computing: Directions for new research challenges”. In 2012 IEEE 36th Annual Computer Software and Applications Conference (pp. 387-394). IEEE..
[18] Butt, S., Lagar-Cavilla, H. A., Srivastava, A., &Ganapathy, V. (2012, October). “Self-service cloud computing”. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 253-264). ACM
[19] Zhu, Y., Hu, H., Ahn, G. J., Han, Y., & Chen, S. (2011, October). Collaborative integrity verification in hybrid clouds. In Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on(pp. 191-200). IEEE.
[20] Ficco, M. (2013).”Security event correlation approach for cloud computing”. International Journal of High Performance Computing and Networking 1, 7(3), 173-185.
[21] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R.,& Molina, J. (2009, November).”Controlling data in the cloud: outsourcing computation without outsourcing control”. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 85-90).ACM.
[22] Gander, M., Felderer, M., Katt, B., Tolbaru, A., Breu, R., &Moschitti, A. (2012, August).“Anomaly detection in the cloud: Detecting security incidents via machine learning”. InInternational Workshop on Eternal Systems (pp. 103-116). Springer Berlin Heidelberg.
[23] Nascimento, G., &Correia, M. (2011, June).“Anomaly-based intrusion detection in software as a service”. In2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)(pp. 19-24). IEEE.
[24] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., &Rajarajan, M. (2013).”A survey of intrusion detection techniques in cloud”.Journal of Network and Computer Applications, 36(1), 42-57.

 