Journal of Information Security, 2015, 6, 142-154
Published Online April 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.62015

A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications

Arif Sari

Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
Email: asari@eul.edu.tr

Received 30 October 2014; accepted 28 March 2015; published 23 April 2015

Abstract

Cloud computing has become one of the most projecting words in the IT world due to its design for providing computing service as a utility. The typical use of cloud computing as a resource has changed the scenery of computing. Due to the increased flexibility, better reliability, great scalability, and decreased costs have captivated businesses and individuals alike because of the pay-per-use form of the cloud environment. Cloud computing is a completely internet dependent technology where client data are stored and maintained in the data center of a cloud provider like Google, Amazon, Apple Inc., Microsoft etc. The Anomaly Detection System is one of the Intrusion Detection techniques. It's an area in the cloud environment that is been developed in the detection of unusual activities in the cloud networks. Although, there are a variety of Intrusion Detection techniques available in the cloud environment, this review paper exposes and focuses on different IDS in cloud networks through different categorizations and conducts comparative study on the security measures of Dropbox, Google Drive and iCloud, to illuminate their strength and weakness in terms of security.

Keywords

Anomaly Detection Systems, Cloud Computing, Cloud Environment, Intrustion Detection Systems, Cloud Security

1. Introduction

Cloud computing is not a promise but a fulfillment in the IT world. The benefits of cloud computing have no in-

How to cite this paper: Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154.
http://dx.doi.org/10.4236/jis.2015.62015

finite end as to what can't be done using the cloud environment due to a variety of deployment model such as Software as a Service, Platform as a Service, and Infrastructure as a Service. The cloud computing technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. This allows flexibility in accessing of data over the cloud network.

Network traffic analysis in cloud environments is one of the most important tasks in cloud management to guarantee the quality of services, validate performance of new applications and services, build accurate network models and detect anomalies in the cloud. The flow of network that is been created by cloud computing systems shows users' behavior in service operation or use. Traffic analysis and the recognition of all significant application flows are important tools for modeling service usage, building up patterns for identifying normal system operations [1].

The cloud computing environment has faced numbers of security challenges. Most of them have been fixed up to an extent, other security aspects spring up and it's vital to know before organizations switch fully. Intrusion detection system in cloud networks plays a very important role as the active security defense against intruders. IDS needs to be employed properly in the cloud networks, because it requires scalability, efficiency and virtualized-based approach in implementation. Sabastian Roschke *et al*. proposed that the users of cloud computing have a limited control over its data and resources that have been hosted on a cloud service provider remote servers [2]. Due to this proposed theory, it automatically becomes the responsibility of the cloud service provider to oversee the IDS in the cloud environment. Additionally, network communication between cloud provider and its customers affects significantly the performance of most cloud-based applications [3]. Analyzing the flow of network traffic provides insights on how applications behave and also their performance in cloud environment. Therefore, it is necessary to develop network traffic measurement and analysis techniques to improve availability, performance and security in cloud computing environments.

On the other hand, managing and analyzing network traffic of large scale cloud systems is a challenging task. The techniques used to monitor and analyze traffic in conventional distributed systems differ from cloud computing systems. In conventional approaches, assumptions are made that network flows follow some patterns, which is acceptable for corporate applications, but cloud applications may have significant changes in traffic patterns [4].

In the first section of this paper the concept of anomaly detection is described and taxonomies of anomalies are discussed broadly. Additionally, separate sections discuss security measures and comparison among basic cloud storage applications such as Google Drive, ICloud and Dropbox to highlight their security preferences and mechanisms.

2. Concept of Anomaly Detection Systems

Anomaly Detection System (ADS) is a technique of the Intrusion Detection System which identifies activities that are not normal among the normality of a system behavior as it is illustrated on **Figure 1** as N represents malicious nodes, R represents routers, G represents anomaly guard modules and "n" represents nodes.

Whenever such anomaly occurs an alert is generated to the administrators that shows the occurrence of an anomaly in the system, this makes a suitable supposition that the anomaly or changes are caused by either malicious or disrupting activities, and the IDS is also capable of suspending or blocking the connection where the anomaly is originating from. The ADS identifies intrusions by classifying activities as either anomalous or normal, and also a training phase needs to be done for the ADS to recognize "new" attacks. The ADS generates more false alarms than the Misuse based IDS systems. The Intrusion Detection System technique is split into two forms or categories which are the Misuse Detection System and the Anomaly Detection System [5].

2.1. Misuse Detection System

Most IDS that are well known make use of the Misuse Detection System approach in the IDS algorithm. The misuse detection system has a pre-defined rules because it works based on the previous or known attacks, that's how intrusion is been detected in the system. It's like the database of an antivirus signature, if it's not up to date it cannot detect new attack signature because such virus signature it's not in its database. The effectiveness of the Misuse Detection System is in detecting only "Know Attacks", because the rules or pattern of the Misuse Detection System are stored in the database of the system. The main downside in the Misuse Detection System is that it doesn't detect new attacks because it's not in its pre-defined rules.

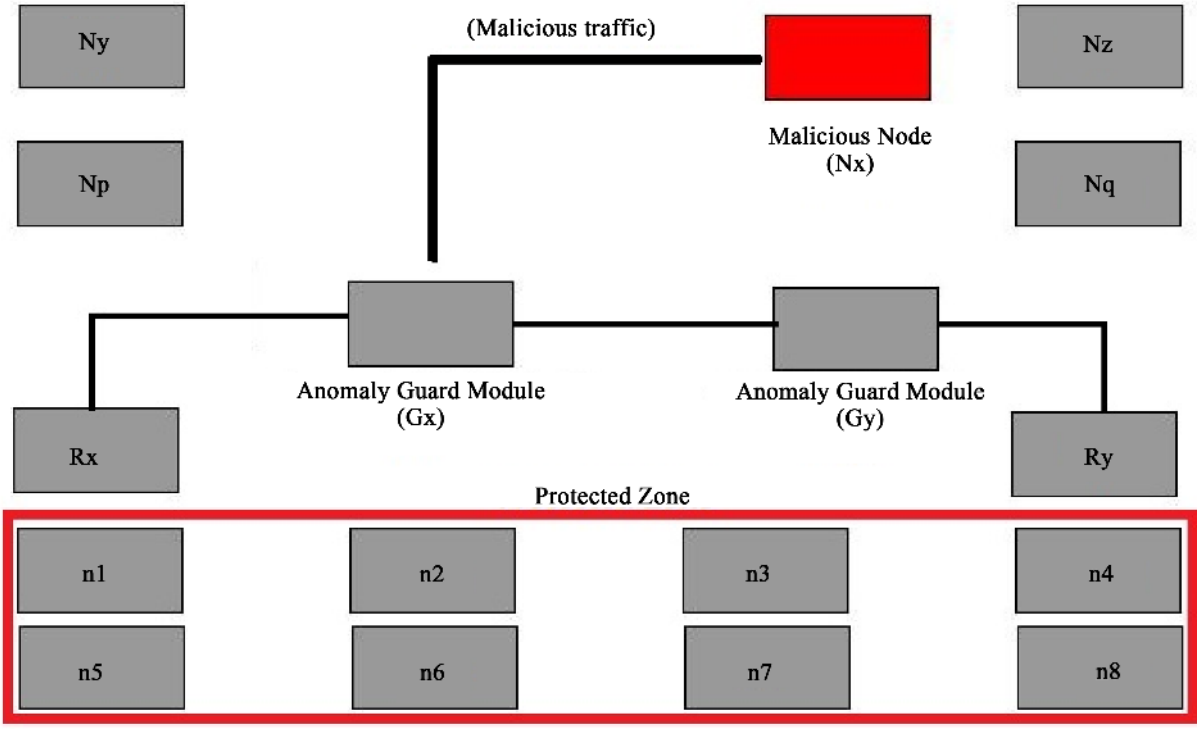

Figure 1. Illustration of anomaly detection.

2.2. Anomaly Detection Systems

There have been studies or research in the Anomaly Detection System in different problem domain, but in the cloud environment it has not been widely researched on. The Anomaly Detection technique in cloud based computing is still in view and evolving because it provides challenges that's still in the cooking pot. Anomaly Detection Systems in cloud based networks detects unwanted traffic in the network and this can be caused by loss of packets, unwanted behavior of application etc.

In a traditional network, IDS monitor detects, and alert the administrative user by deploying IDS on important points on the user site. But in the cloud network IDS has to be managed by the service providers [6]. The data that the intrusion communicates through is passed through the cloud service provider, this makes it only possible for the service provider to be the administrator and the user just has to depend on the service provider. Most times the user is not aware of such activities so as to keep the reputation and image of the cloud service provider. A solution was proposed by Roschke and *et al*. [2] that combines and integrates various IDS sensor output reports on a single interface. The communication between different IDS has been with the Intrusion Detection Message Exchange Format (IDMEF) standards. The positioning of IDS sensors on various layers of the cloud environment like the application layer, system layer, and platform layer can create better communication between the IDS sensors and also increases the detection process within the cloud environment. Generated prompts or alerts are sent to the "Event Gatherer" program. The Event Gatherer program acts as a collector of alerts that spring up as a result of intrusion in the cloud based network. The alert received by the Event Gatherer is converted in the IDMEF standard and is stored in the Event Gatherer database with the help of a plug-in known as the Sender and Receiver Handler plug-in [7].

3. Taxonomy of Anomalies

Anomaly detection aspires at finding the presence of anomalous patterns in network traffic and usual detection of such outline can provide network administrator with extra information source to identify network behavior or tracing and locating the root cause of faults in a network [8]. Anomalies can be classified into three categories: as Point Anomalies, Contextual Anomalies and Collective Anomalies [9] [10].

3.1. Point Anomalies

This is when an individual data instance deviates from its normal activity or form it is said to be anomalous, because other data are normal. This shows that the anomalous activity lies outside the boundaries of the normal region. This is the easiest type of anomaly amongst the 3 types or categories and it is the strength or importance of anomaly detection. **Figure 2** illustrates the point anomalies.

From **Figure 2**, N_1 and N_2 are regions of normal behavior, Points O_1 and O_2 are anomalies and Points in region O_3 are anomalies.

3.2. Contextual Anomalies

The contextual anomalies occur when the occurrence of information is or shows traces of anomalous character in an exact or precise context, which is the unwanted behavior of activities that surrounds an individual data instance. **Figure 3** illustrates the Contextual Anomaly.

As it is shown on **Figure 3**, when this occurs it is characterized as a related anomaly. This requires an idea or notion of context in the data instance. It is also referred to as conditional anomalies.

3.3. Collective Anomaly

This is when related data instances collected acts as anomalous or show unwanted activities related to the entire data set. In collective anomaly, the individual data instance with collective anomaly are not otherwise said to be anomalous on their own because the collective anomaly requires a relationship between or among data instances; Sequential, Spatial, and Graph data to cause a collective anomaly. But their occurrence as a whole or collection is or can be anomalous. **Figure 4** illustrates the Collective anomaly.

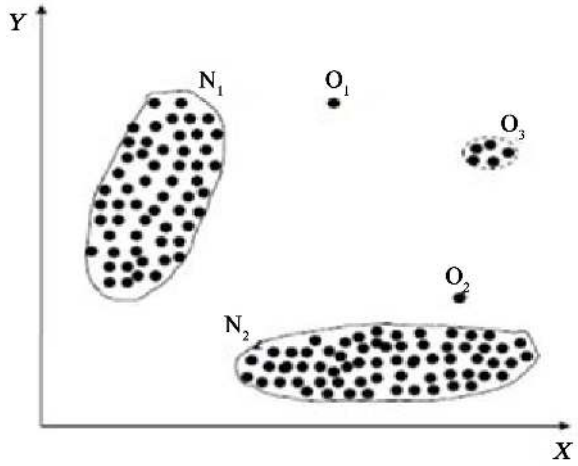

Figure 2. Illustration of point anomaly.

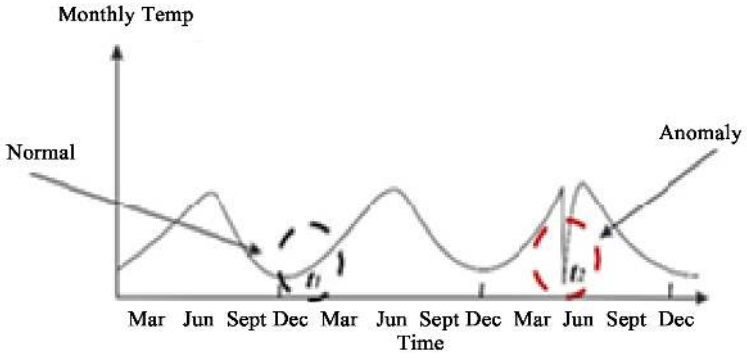

Figure 3. Illustration of contextual anomaly.

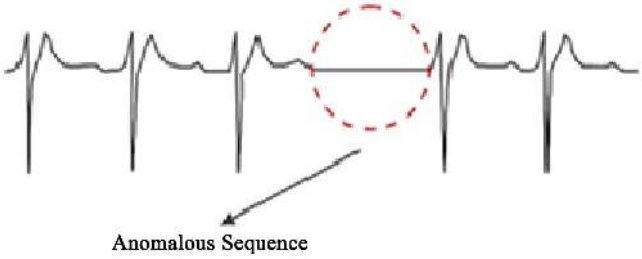

Figure 4. Collective anomaly.

4. Anomaly Detection in Cloud Networks

In cloud networks, traffic or flow of packets comes from more than one domain. There's a rapid change that occurs in the cloud environment due to the patterns or behavior of clients/tenants using the cloud infrastructure and the state of the unprotected services. In cloud environment, various challenges of identifying anomaly detection such as misconfiguration or high volumes of legitimate traffic in the network. The importance of the anomaly detection in cloud networks is the unwanted activities in data that brings the importance of reason for such anomaly in the information. Generally, the commercial off-the-shelf systems (COTS) for detecting intrusions are based on signatures or rules [11] [12].

Signature based IDS can be used to detect known attacks in the cloud network, although the point of deploy can be before the cloud to detect external or incoming attacks or at the back end of the cloud to detect both external and internal attacks.

4.1. Methods and Techniques of Anomaly Detection in Cloud Based Networks

In the cloud networks, there are different techniques or methods that have been used in the detection of anomalous activities; these include Threshold detection, statistical analysis, Rule-based measures, neural networks, genetic algorithms, data mining and machine learning [13]. This section exposes a comparative view of the different method of anomaly detection in cloud networks. A comparison between the three main methods or techniques and others would be researched on namely; Statistical, data mining and machine learning.

4.1.1. Statistical Anomaly Detection Systems

This method of anomaly detection in cloud base network detects anomaly by observing computations in the network and creates a profile which keeps or stores the generated value in resenting their behavior. In identification of anomaly using this technique, there are two profiles created; the first one stores the normal or anomaly rules or signatures while the second one updates at regular intervals. During the update anomaly scores are calculated. If the threshold value is lower than the current anomaly profile generated, then it is known to be anomalous and detected. There's high probability of occurrence of normal data instances in dense regions of the model, while irregularities is seen in the low possibility regions [14]. Some proposed model of Statistical Anomaly Detection Systems are: Cloud Diag [15], EbAT (Entropy based Anomaly Testing) [16] etc.

The benefits of using this technique are that there is no previous or prior knowledge or training of security risks or knowledge domain required. Additionally, it has the capability of detecting even recent anomaly generated in the network or data and there's accurate notification of anomalies that have occur over extended time frame.

4.1.2. Data Mining Based Anomaly Detection Systems

The analyzing or extracting knowledge of large data set to fine patterns that are useful to the data owner is known as Data Mining [17] [18]. This technique uses the classification, clustering and association rule mining methods in the detection of anomalies in cloud environment. An analyst mechanism is in the data mining technique that detects anomaly by differentiating between normal and abnormal activities within the cloud. This is accomplished by stating or delineating some boundaries for valid and normal activities in the cloud network. There's also an added level of focus in this technique for anomaly detection. Data mining techniques are more flexible and easily to deploy at any point. Putting data mining into effect in the cloud network makes available the opportunity to extract meaningful information from data warehouse that are integrated into the cloud, this

reduces the infrastructure storage costs. Customers or users of a cloud service only have to pay for the data mining tool that's been used [19].

Data mining is typically used by Cloud Service Providers to provide a much better service for their users or clients using their cloud service [19]. The downside in this is that if the clients are not informed of the information that's been collected and used for mining, there's a violation of their privacy and it's illegal. There are varieties of issues available in data mining detection in cloud based networks which are the priority replacement of preserving privacy and setting the wrong parameters of these privacy settings while using different rules and strategy to enhance cloud network security.

4.1.3. Machine Learning Based Anomaly Detection Systems

The ability for programs or software to improve performance of their task over time by learning is an important technique in the detection of anomaly. Verified values or normal behavior of data are stored, when anomaly occurs or is being detected the machine learns its behavior, stores the new sequence or rule. This technique creates a system that can improve on performance of the program by leaning from the previous results. The interesting part in this technique is that upon improving of performance from previous results, new information are extracted and if it requires a change in the strategy of execution to improve performance it is done on the basis of the new information from the previous results. There are various categories of Machine leaning based anomaly detection such as; Bayesian Network, Genetic Algorithm, Neural Network etc.

Bayesian Network has the ability to include in its process both the old knowledge or signature and the data in detecting of anomalies. This technique is combining with the statistical mechanism which is highly advantageous in anomaly detection [20].

Neural Networks has the capability to improve on data that is not complete to create a potential to detect and understand patterns that are not visible. The Neural network does not only detect previous attacks but also unseen behavior or patterns [21]. Genetic Algorithms employs the evolutionary algorithm techniques such as mutation, selection etc. their different process is based on collected rules from the information on the network analysis carried out by the IDS.

4.1.4. Adaptive Anomaly Detection Systems

The Adaptive Anomaly Detection Systems (AAD) employs data description using hyper-sphere for adaptive failure detection. In cloud networks, possible failures or anomaly which are detected by cloud operators are detected by the AAD using the performance data of the cloud service. The AAD detection systems utilize or capitalize on the log of the detected failure records that have been sent in by the cloud operators to identify new types of failures subsequently. The AAD detection algorithm changes its behavior by repeatedly learning from the new certified results or detection from the cloud provider so as to be prepared for future detections. According to Husanbir S. Pannu *et al.* [22] a prototype of AAD system was built and experiment was conducted in it testing the prototype in a 362-node cloud computing environment.

It was noted that the prototype was lightweight, and it took couple of seconds to startup the detector and couple of seconds more for the set adaptation and the failure detection to be up and running. 518 metrics were profiled every minute, the profiling covered or circled through the entire statistics of a typical cloud server, its Central Processing Unit usage, task switching processes, memory and swap space utilization, paging and page faults, input and output data transfer, interrupts, and more. Failure detector such as subspace regularization was used in comparing the ADD algorithm. The failure detector in [23] achieves 67.8% sensitivity in the experiments. The Bayesian sub-models and decision tree classifiers that were proposed only have 72.5% detection sensitivity. In the AAD the failure detector could get up to 92.1% and 83.8% detection sensitivity and detection specificity [22].

As shown on **Figure 5**, to make failure detection it takes 7.26 seconds on an average control node in the cloud network, to extract the performance metrics, create the hyper sphere and make failure detections. It is even more lightweight in updating of the hyper sphere and identifies failures in about 2.17 seconds.

5. Comparative Survey of Cloud Security Measures in Cloud Storage Applications

Cloud storage is a useful way of storing data and also sharing of information online. The important question asked is "is it safe to store sensitive information on the cloud?" well that's a question we are trying to evaluate

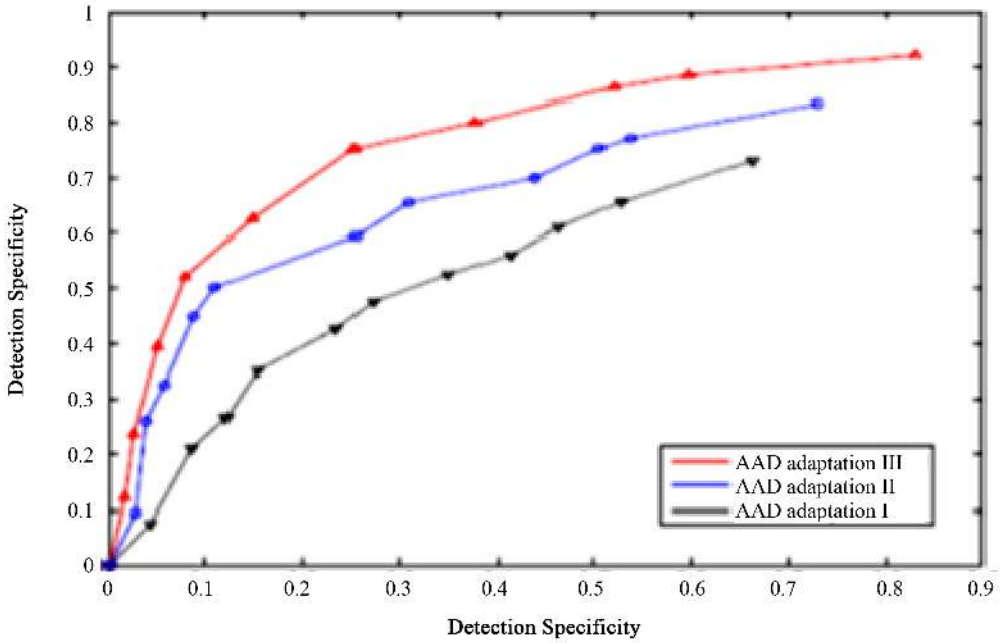

Figure 5. Illustration of failure detection with AAD.

and answer if possible. Security in the cloud is not all that 100% guarantee. Files maybe encrypted in transmission, and at the final destination, the CSP might decrypt the file to gain access because the encryption algorithm used is provided by them. Access to your account can be gotten by anyone and your sensitive files can be compromised. In this case encryption on the client or the cloud user side is important and also using of a strong encryption key is advised.

In cloud computing, the usability of the computing capabilities have been moved from the users side to that of the CSP end; meaning users can access their files from anywhere at any time even using of multiple devices such as laptops, tablets, smart phones etc. this gives the user a sense of data mobility than just storing the data in a computer at home only [20].

5.1. Dropbox

Dropbox is a public cloud storage, which was developed by 2 graduate of MIT who always forget or misplace their USB devices holding information that they need to use momentarily. Due to this Dropbox was brought to light in the IT world. In 2007 Dropbox Inc. was founded, it provides cloud storage, client software and file synchronization [21]. Dropbox allows it users to upload their files or folders into the Dropbox folder where it can be viewed or shared on any device at any time as long as the device has Dropbox installed along with a username and password and also internet connection for synchronization.

Dropbox was developed for personal use that was the intention of the two MIT graduate, but as of 2011 the cloud application have housed over 50 million users worldwide storing over 20 billion files and occupying petabyte of storage. Dropbox gives a 2 GB cloud storage space for free, but additional space can be purchased. Dropbox application is available for windows, Apple OS X, Android, and Linux [21].

Figure 6 illustrates the example of working mechanism of Dropbox protocol. The basic mechanism is working based on so called hand-shaking process of basic networking standards.

Dropbox Security Measures

The cloud computing environment has many security issues affecting its usability. Dropbox being a cloud application or storage has several security measures put in place to ensure the data integrity and data security is in check. Dropbox saves all deleted and earlier versions of files for thirty days; this feature is supported by both the free and the premium (that's the paid account) account. In the free account the "save earlier version of files" feature only apply for 30 days, while in the paid or premium account the features saves the files indefinitely. The

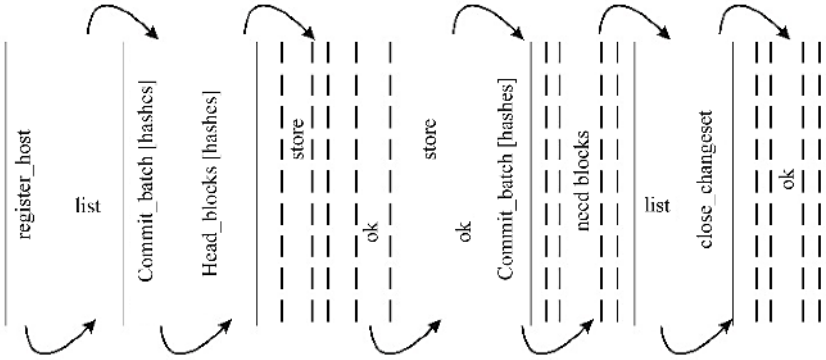

Figure 6. Illustration of Dropbox protocol.

Amazon S3 (Simple Storage Service) is used in the Dropbox cloud computing environment for their file storage. This is done for high integrity and data availability, and multiple data center replication is also used [14].

An AES-256 encryption is used for ensuring privacy of data in the Dropbox cloud environment. In Dropbox, encryption is machine-protected that is the encryption key is stored in the machine not in the cloud storage [14]. Additionally the Dropbox encryption algorithm uses a TEA symmetric encryption [15].

The SSL secure tunnel protocol is utilized for data in transit, and it's also an AES-256 encryption standard. Two-step verification process is used for or to increase security measures and it is recommended [15] [16]. Availability of third-party applications in the Dropbox cloud environment also adds another form of security in data encryption [15] [16]. Additionally Dropbox uses SQLite 3 database for ensuring data integrity and no data redundancy when users communicate with the database. The network traffic is fully transported over HTTPS, Proper certificate checking is done during the authentication process and OpenSSL is used to tackle with security issues in Dropbox services [17].

The usage of OpenSSL increase security for authentication and authorization of Dropbox users. NCrypt wrapper is used by the Dropbox. The NCrypt wrapper creates security where there's none. The NCrypt is a file encyptor/decryptor and uses AES as its encryption algorithm [17] [18].

It minimizes the exposure of plaintext password in memory and converts the plaintext to a SHA-1 hash before erasing the plaintext from hard drive immediately, and once the SHA-1 is used to make a key for encryption it is wiped form the memory too [17]-[19]. RSYNC (Remote Synchronization) Protocol is used, which allows a user to synchronize files between two or more computer device making sure that the same file is available in all connected device. Remote device unlinking is another technology used in Dropbox [24].

5.2. Google Drive

The "Google Drive" is the Google version of cloud storage, and it is one of the popular cloud services. It supports photos, videos, documents and other files. There's a 15 GB free storage given that can be increased at any time by the user. Google drive provides generic applications for viewing of more than 30 file types without having to install the corresponding application into your computer system for viewing the corresponding file type. The Google drive provides unlimited file size upload quotation for uploading files into corresponding user drive.

Google Drive Security Measures

The Google Drive is integrated into Gmail services and once user owns a Gmail account can automatically have a Google drive account setup. Since Google drive uses a 2 step verification feature, the data security becomes one of the important obstacles for the corresponding technology users since 3-tier security architectures are more important and enhance data security for users [25]-[27].

Additionally, "Cloud lock" feature is used to improve personal security of information and this also ensures PCI compliance. Files in Google drive are encrypted using AES-256 and RSA-4096 standards and in addition to his, there is an automatic data encryption on Google drive and server-side encryption mechanisms are used [28] [29].

5.3. iCloud

iCloud is cloud storage from Apple Inc. It was launched on October 12, 2011 [30]. iCloud offers its users with the means to store data such as; documents, images, videos, etc. users can also backup their iOS devices directly to the iCloud wirelessly. As of July 2013, the iCloud service had 320 million users [31] [32]. The iCloud was first branded as iTools in 2000, Mac in 2002, and MobileMe in 2008 [32].

iCloud Security Measures

iCloud keeps data of its users secure by encrypting it when it is sent over the Internet or in transition which also contains 2 step verification processes [33]. Secure tokens are used for authentication, this creates a secure and unauthorized access both in transit and while it is stored in the iCloud. For the messages transferred over the network, iCloud introduced iCloud Keychain, which uses a 256-bit AES encryption to store password and also to store credit card information. It uses elliptic curve asymmetric cryptography and key wrapping. The iCloud Keychain encryption keys are created and stored on the user's device not on the iCloud server [34] [35]. iCloud sessions are encrypted with SSL protocol to enhance security for login information and a minimum of 128-bit AES encryption is used for encrypting documents in iCloud. The files that will be transferred are encrypted in transition using 128-bit AES encryption algorithm [36].

6. Comparison of Cloud Services: iCloud, Dropbox and Google Drive

The various cloud services that this paper is characterized on, having their various service requirements to their clients as well as their cost. In **Table 1**, a detailed comparison was carried out to determine which among the three cloud services has a better security feature. We'd find out that the Dropbox cloud service incorporate more security measure compared to the Google Drive and iCloud.

Dropbox cloud storage service accounts for about 100 GB of traffic daily in one of their networks that was monitored [37]. A deduplication mechanism was developed to help avoid the duplication of data [38] [39]. Dropbox has the sharing of content ability and the percentage of files or folder shared amongst home users is about 70%, while linked devices is about 30%. Amongst students in campus about 40% of them share 5 folders or more. Dropbox uses delta encoding mechanism when transferring or transmitting chunks, "a chunk is a split large file". In Dropbox, a file larger than 4 MB is split into chunks which are identified by a SHA256 hash value, which is included in the meta-data description of files [40].

The two major components in the Dropbox architecture that can be identified are the control and data storage [37]. In Dropbox cloud service, each linked device has a unique identifier (host_int), these unique identifier are also used for each shared folder in Dropbox. The various devices that belong to a single user are deduced by re-lating namespace lists [40].

Table 1. Secuirty comparison between Dropbox, Google drive, and iCloud.

Security Measures	Google Drive	Dropbox	iCloud
Secure Connection	YES	YES	YES
Files Stored Encryption	YES	YES	YES
SSL Protocol	YES	YES	YES
Open SSL	NO	YES	NO
128-bit AES encryption Algorithm	NO	NO	YES
2-step Authentication process	YES	YES	YES
HTTPS protocol	YES	YES	YES
Remote Device Unlinking	NO	YES	NO
AES-256 Encryption	NO	YES	YES
RSYNC (Remote Synchronization)	YES	YES	YES
NCrypt Wrapper	NO	YES	NO

Contents that are stored in Dropbox can be viewed and accessed using a web interface like a browser. Different set of domain names are used to identify public and private operations; URLs that contain dl-web.dropbox.com are associated with the private contents, while the dl.dropbox.com is associated with the public shared files [37].

Google Drive is best for creating of documents and sharing of files. You can create spreadsheets, presentations, drawing, a new document etc. and stored files can be accessed anywhere with smartphones having Google Drive apps installed and desktop applications are available for PCs and Mac. Synchronization of files between PC and Google Drive is done automatically [37].

As it is shown on **Figure 7**, Google Drive supports Microsoft Word documents, PowerPoint presentations, Adobe InDesign, Adobe Illustrator, Microsoft Excel, Adobe Photoshop, Wave Audio files, Adobe Reader, etc. with these applications installed in the Google Drive by the cloud service provider, it makes it may easy for users to edit, create and view respective documents without having to install corresponding application on every device.

In **Table 1** shown, the various security measures of the Dropbox, Google Drive, and iCloud shows that the security infrastructure of various cloud services differs in the perspective of data security, availability, and control.

In **Table 2**, Dropbox gives 2 GB of free storage to a subscribed user of its cloud services; additional storage space can be added by buying a premium package. Google Drive gives 15 GB free storage space to its users, also additional storage can be purchased to increase the storage capacity, finally iCloud gives 5 GB free storage to its users and additional storage is available to users for a price. For users going for a free large storage capacity Google Drive has a better offer. Dropbox, Google Drive and iCloud allow any file type to be stored in their cloud server by their clients. Offline feature is also available so users can download a file to view later even when there's no internet connection.

Dropbox, Google Drive and iCloud allow any file type to be stored in their cloud server by their clients. Offline feature is also available so users can download a file to view later even when there's no internet connection.

As it is shown in **Table 3**, the cloud services differ also in terms of price, storage and performance. **Table 3** shows the price difference in services of Dropbox, Google Drive, and iCloud. However, it depends on the user and its choice of product.

Table 4 indicates the overall capability of Cloud storage applications. As it can be seen from the table, the Dropbox is the only cloud storage application that allows all features while iCloud and Google Drive does not.

Figure 7. Generic applications of Google drive.

Table 2. Storage comparison between Dropbox, Google drive, and iCloud.

	Dropbox	Google Drive	iCloud
Storage Space	2 GB	15 GB	5 GB
Maximum File Space	N/A	250 MB	N/A
File Type	Anything	Anything	Anything
Offline Services	YES	YES	YES

Table 3. Service cost of Dropbox, Google drive, and iCloud.

Storage	Dropbox	Google Drive	iCloud
100 GB	$99	$60	N/A
200 - 250 GB	N/A	$120 (200 GB)	$3.99 (200 GB)/month
400 - 500 GB	$499 (500 GB)	$240 (400 GB)	$9.99 (500 GB)/month
1 TB	$119.99	$600	$19.99/month
2 - 16 TB	N/A	$1200 - 7600	N/A

Table 4. Capability measures of Dropbox, Google drive, and iCloud.

Capability	Dropbox	Google Drive	iCloud
Chunking	YES (4 MB)	YES (8 MB)	NO
Bundling	YES	NO	NO
Client-Side Deduplication	YES	NO	NO
Data Encoding	YES	NO	YES
Data Compression	YES	YES	NO

7. Conclusion

Anomaly detection in could networks is a wide area of research, and it holds a good number of developments and proposing of detection systems. Anomalous activities occur always in our networks cloud based or non-cloud based. With the different types of methods or techniques in anomaly detection in cloud based network, detection of unwanted behavior can be traced, detected, stopped. These techniques have their limitations that create a gap between their performance metrics. In cloud based network hybrid anomaly detection system or method should be used so as to have a more efficient and high performance system. In this paper, we have discussed the importance of anomaly detection system in cloud environment, its types, methods, and the limitations that each method is faced with such as, false alarm being created; detection accuracy is hinged on the basis of previous collected information on anomalous behavior; more time is needed in the identification of attacks etc. These limitations can create inaccuracy in anomaly detection. A wide study should be conducted to develop a more reliable and efficient model that would encompass and try to improve on the limitations that are associated to the anomaly detection systems. Security in the cloud computing environment is very important as individuals and companies utilize their services. In this paper we have compared the security measures of Dropbox, Google Drive, and iCloud; we have found that most of the cloud service providers have similar security measures while few are different. Some of their similarities are the use of AES encryption algorithm, the communication over HTTPS, the use of SSL protocol, and the 2-step authentication process. This helps to secure data both in transit and in the cloud storage. Dropbox security measures tend to be intense in protecting the information of its cloud users; it incorporates Ncrypt wrapper and the Remote Device Unlinking mechanism. From the security measures, I'd say that for a more secured cloud service the Dropbox is a best choice although you can increase the storage by going for the premium offer which is costly, but for storage and application variety the Google Drive is a take.

References

[1] Oliveira, A.C., Chagas, H., Spohn, M., Gomes, R. and Duarte, B.J. (2014) Efficient Network Service Level Agreement Monitoring for Cloud Computing Systems. 2014 *IEEE Symposium on Computers and Communications* (*ISCC*), Funchal, 23-26 June 2014, 1-6.

[2] Roschke, S., Cheng, F. and Meinel, C. (2009) Intrusion Detection in Cloud. *Eight IEEE International Conference on Dependable Automatic and Secure Computing*, Liverpool, 729-734.

[3] Zhang, Q., Cheng, L. and Boutaba, R. (2010) Cloud Computing: State-of-the-Art and Research Challenges. *Journal of Internet Services and Applications*, **1**, 7-18. http://www.springerlink.com/index/10.1007/s13174-010-0007-6

[4] Wang, C. (2009) Ebat: Online Methods for Detecting Utility Cloud Anomalies. *Proceedings of the* 6*th Middleware Doctoral Symposium*, ser. MDS '09. New York, ACM, 4:1-4:6. http://doi.acm.org/10.1145/1659753.1659757

[5] Hussain, M. (2011) Distributed Cloud Intrusion Detection Model. *International Journal of Advanced Science and Technology*, **34**, 71-82.

[6] Gul, I. and Hussain, M. (2011) Distributed Cloud Intrusion Detection Model. *International Journal of Advanced Science and Technology*, **34**, 71-81.

[7] Shelke, P.K., Sontakke, S. and Gawande, A.D. (2012) Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research*, **1**, 67-71.

[8] Denning, D.E. (1987) An Intrusion Detection Model. *IEEE Transactions on Software Engineering*, Vol. SE-13, 222-232.

[9] Marhas, M.K., Bhange, A. and Ajankar, P. (2012) Anomaly Detection in Network Traffic: A Statistical Approach. *International Journal of IT*, *Engineering and Applied Sciences Research* (*IJIEASR*), **1**, 16-20.

[10] Gu, Y., McCallum, A. and Towsley, D. (2005) Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation. *Proceedings of Internet Measurement Conference*, October 2005.

[11] IBM Security Network Intrusion Prevention System. Technical Report. http://www-01.ibm.com/software/tivoli/products/security-network-intrusion-prevention/

[12] Cisco Intrusion Prevention System. Technical Report, Cisco.

[13] Cisco Network Solutions, 2015. http://www.cisco.com/go/ips

[14] Hand, D.J., Mannila, H. and Smyth, P. (2001) Principles of Data Mining. The MIT Press, Cambridge.

[15] Wu, X., Kumar, V., Ross Quinlan, J., Ghosh, J., Yang, Q., Motoda, H., *et al.* (2008) Top 10 Algorithms in Data Mining. *Knowledge and Information Systems*, **14**, 1-37. http://dx.doi.org/10.1007/s10115-007-0114-2

[16] Pannu, H.S., Liu, J.G. and Fu, S. AAD: Adaptive Anomaly Detection System for Cloud Computing Infrastructures.

[17] Garcia Teodora, P., Diaz Verdejo, J., Macia Farnandez, G. and Vazquez, E. (2009) Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. *Computers & Security*, **28**, 18-28. http://dx.doi.org/10.1016/j.cose.2008.08.003

[18] Zhang, Y.M., Hou, X., Xiang, S. and Liu, C.L. (2009) Subspace Regularization: A New Semi-Supervised Learning Method. *Proceedings of European Conference on Machine Learning and Knowledge Discovery in Databases* (*PKDD*), Bled, 7-11 September 2009, 586-601. http://dx.doi.org/10.1007/978-3-642-04174-7_38

[19] Alsafi, H.M., Abduallah, W.M. and Khan Pathan, A. (2012) IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment. *International Journal of Computing and Information Technology* (*IJCIT*).

[20] Mi, H.B., Wang, H.M., Zhou, Y.F., Lyu, M.R.T. and Cai, H. (2013) Toward Fine-Grained, Unsupervised, Scalable Performance Diagnosis for Production Cloud Computing Systems. *IEEE Transactions on Parallel and Distributed Systems*, **24**, 1245-1255. http://dx.doi.org/10.1109/TPDS.2013.21

[21] Wang, C.W., Talwar, V., Schwan, K. and Ranganathan, P. (2010) Online Detection of Utility Cloud Anomalies Using Metric Distributions. *IEEE Network Operations and Management Symposium* (*NOMS*), Osaka, 19-23 April 2010, 96-103.

[22] Chandola, V., Banerjee, A. and Kumar, V. (2009) Anomaly Detection: A Survey. *ACM Computing Surveys*, **41**, 1-58.

[23] Han, S.J. and Cho, S.B. (2006) Evolutionary Neural Networks for Anomaly Detection Based on the Behavior of a Program. *IEEE Transaction on Systems*, *Man*, *and Cybernetics*, *Part B*: *Cybernetics*, **36**, 559-570.

[24] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009) Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. *Future Generation Computer Systems*, **25**, 599-616. http://dx.doi.org/10.1016/j.future.2008.12.001

[25] Sara, T., Vance, C., Fenger, T., Brunty, J. and Price, J. (2013) Forensic Analysis of Dropbox Application File Artifacts Recovered on Android and iOS Mobile Devices.

[26] Bermudez, I., Mellia, M., Munafo, M.M., Keralapura, R. and Nucci, A. (2012) DNS to the Rescue: Discerning Content and Services in a Tangled Web. *Proceedings of the* 12*th ACM SIGCOMM Conference on Internet Measurement*, *IMC*'12, Boston, 14-16 November 2012, 413-426. http://dx.doi.org/10.1145/2398776.2398819

[27] Ruff, N. and Ledoux, F. A Critical Analysis of Dropbox Software Security.

[28] Wallen, J. (2014) Easy Steps for Better Google Drive Security. www.techrepublic.com/article/easy-steps-for-better-google-drive-security

[29] www.hongkiat.com/blog/dropbox-gdrive-skydrive/

[30] Singh, J. and Jha, A. (2014) Cloud Storage Issues and Solutions. *International Journal of Engineering and Computer Science*, **3**, 5499-5506.

[31] Barth, D. (2013) Google Cloud Storage now Provides Server-Side Encryption. www.googlecloudplatform.blogspot.com/2013/08/google-cloud-storage-now-provides.html

[32] GBacom News. http://GBaom.com/apple/apple-may-have-snapped-up-icloud-com

[33] CNET News. http://news.cnet.com/8301-13579_3-20068165-37.html

[34] Computerworld Report Articles, on iCloud. http://www.computerworld.com/s/article/9216301/Reports_Apple_acquires_icloud.com_domain

[35] Voo, B. (2014) Cloud Storage Face-Off: Dropbox vs Google Drive vs SkyDrive. http://www.hongkiat.com/blog/dropbox-gdrive-skydrive/

[36] http://www.whois.net/whois/icloud.de

[37] Marshall, G. (2014) Best Cloud Services Compared: Google Drive vs OneDrive vs Amazon vs iCloud vs Dropbox. http://www.techradar.com/news/internet/cloud-services/best-cloud-storage-dropbox-vs-skydrive-vs-google-drive-vs-icloud-1120024/2#articleContent

[38] Drago, I., Mellia, M., Munafo, M.M., Sperotto, A., Sadre, R. and Pras, A. (2012) Inside Dropbox: Understanding Personal Cloud Storage Services. *Proceedings of the* 12*th ACM Internet Measurement Conference*, *IMC*'12, Boston, 14-16 November 2012, 481-494. http://dx.doi.org/10.1145/2398776.2398827

[39] Halevi, S., Harnik, D., Pinkas, B. and Shulman-Peleg, A. (2011) Proofs of Ownership in Remote Storage Systems. *Proceedings of the* 18*th ACM Conference on Computer and Communications Security*, *CCS*'11, Chicago, 17-21 October 2011, 491-500. http://dx.doi.org/10.1145/2046707.2046765

[40] Harnik, D., Pinkas, B. and Shulman-Peleg, A. (2010) Side Channels in Cloud Services: Deduplication in Cloud Storage. *IEEE Security and Privacy*, **8**, 40-47. http://dx.doi.org/10.1109/MSP.2010.187