The American Journal of Engineering and Technology
(ISSN – 2689-0984)
Published: February 28, 2021 | Pages: 140-157
Doi: https://doi.org/10.37547/tajet/Volume03Issue02-20

IMPACT FACTOR
2021: 5. 705
OCLC - 1121105677

An Overview Of Anomaly Detection Systems In Cloud Networks And An Overview Of Security Measures In Cloud Storage

O'rinov Nodirbek Toxirjonovich
Teacher, Department Of Information Technology, Andijan State University, Uzbekistan

Abdullayev Elmurod Zaylobiddinovich
Teacher, Department Of Information Technology, Andijan State University, Uzbekistan

Abdujabborov Madaminjon Vohidjon O'g'li
Teacher, Department Of Information Technology, Andijan State University, Uzbekistan

ABSTRACT

Cloud computing has become one of the loudest words in the IT world because of its design to deliver computing services as a utility. The typical use of cloud computing as a resource has changed the computing landscape. Increased flexibility, reliability, scalability and lower costs have attracted the attention of both companies and individuals due to the form of payment for using the cloud. Cloud computing is a completely internet-dependent technology in which customer data is stored and served in the data center of a cloud provider such as Google, Amazon, Apple Inc., Microsoft etc. Anomaly detection system is one of the intrusion detection methods. It is an area of the cloud environment designed to detect unusual activity in cloud networks. While there are various intrusion detection methods available in the cloud, this white paper explores and explores the various IDSs in cloud networks by different categories, and compares the security measures of Dropbox, Google Drive, and iCloud to clarify their strengths and weaknesses. in terms of security.

KEYWORDS

Anomaly detection systems, cloud computing, cloud environment, intrusion detection systems, cloud security

INTRODUCTION

Cloud computing is not a promise, but an implementation in the IT world. The benefits of cloud computing are not unlimited in terms of what cannot be done using the cloud due to different deployment models such as Software as a Service, Platform as a Service and Infrastructure as a Service. Cloud computing technology can dramatically improve computing efficiency by centralizing storage, memory, processing, and bandwidth. This provides the flexibility to access data over the cloud.

Analyzing network traffic in cloud environments is one of the most important tasks in cloud management to ensure service quality, validate the performance of new applications and services, build accurate network models, and detect anomalies in the cloud. The network flow generated by cloud computing systems shows the behavior of users when operating or using a service. Traffic analysis and recognition of all significant application flows are important tools for modeling the use of services, building templates for determining normal system operations [1].The cloud computing environment has faced a number of security challenges. Most of them have been fixed in some way, and there are other security aspects that are important to be aware of before organizations completely switch. Cloud intrusion detection systems play a very important role as active defense against intruders. IDS needs to be used correctly in cloud networks because it requires scalability, efficiency, and a virtualized approach to implementation. Sabastian Roschke and others. suggested that cloud computing users have limited control over their data and resources, which are hosted on remote servers of the cloud provider [2]. According to the proposed theory, the cloud provider automatically becomes the responsibility to monitor the IDS in the cloud. In addition, the network communication between the cloud service provider and its customers significantly affects the performance of most cloud applications [3]. Analyzing network traffic flow provides insight into the behavior of applications as well as their performance in the cloud. Consequently, methods for measuring and analyzing network traffic need to be developed to improve availability, performance, and security in cloud computing environments.

On the other hand, managing and analyzing the network traffic of large-scale cloud systems is challenging. The methods used to monitor and analyze traffic in conventional distributed systems are different from cloud computing systems. Traditional approaches assume that network flows follow some patterns, which is acceptable for corporate applications, but cloud applications can have significant changes in traffic patterns [4].

The first section of this article describes the concept of anomaly detection and discusses anomaly taxonomies extensively. Additionally, separate sections discuss security measures and compare major cloud storage applications such as Google Drive, iCloud and Dropbox to highlight their security preferences and mechanisms.

2. The concept of detecting system anomalies

Anomaly Detection System (ADS) is an intrusion detection system technique that detects actions that are not normal for normal system behavior, as shown in Figure 1, since N represents malicious nodes, R represents routers, and G represents anomaly protection modules. and "n" represents nodes.

Whenever such an anomaly occurs, an alert is generated for administrators that indicates the occurrence of an anomaly in the system, this makes a reasonable assumption that the anomaly or changes are caused by either malicious or disruptive activity, and IDS can also suspend or block the connection from which the anomaly originated ... ADS identifies intrusions by classifying actions as abnormal or normal, and a training step is required to enable ADS to recognize "new" attacks. ADS generates more false alarms than misuse-based IDS systems. Intrusion detection system technique is divided into two forms or categories: misuse detection system and anomaly detection system [5].

2.1. Misuse detection system

Most of the well-known IDS use a misuse detection system approach in the IDS algorithm. The misuse detection system has predefined rules because it works on the basis of previous or known attacks, this is how intrusion is detected in the system. This is similar to the antivirus signature database: if it is not updated, it cannot detect a new attack signature because no such virus signature is in its database. The effectiveness of a misuse detection system is to detect only “known attacks” because the rules or pattern of the misuse detection system is stored in the system database. The main disadvantage of the misuse detection system is that it does not detect new attacks, because it is not in its predefined rules.

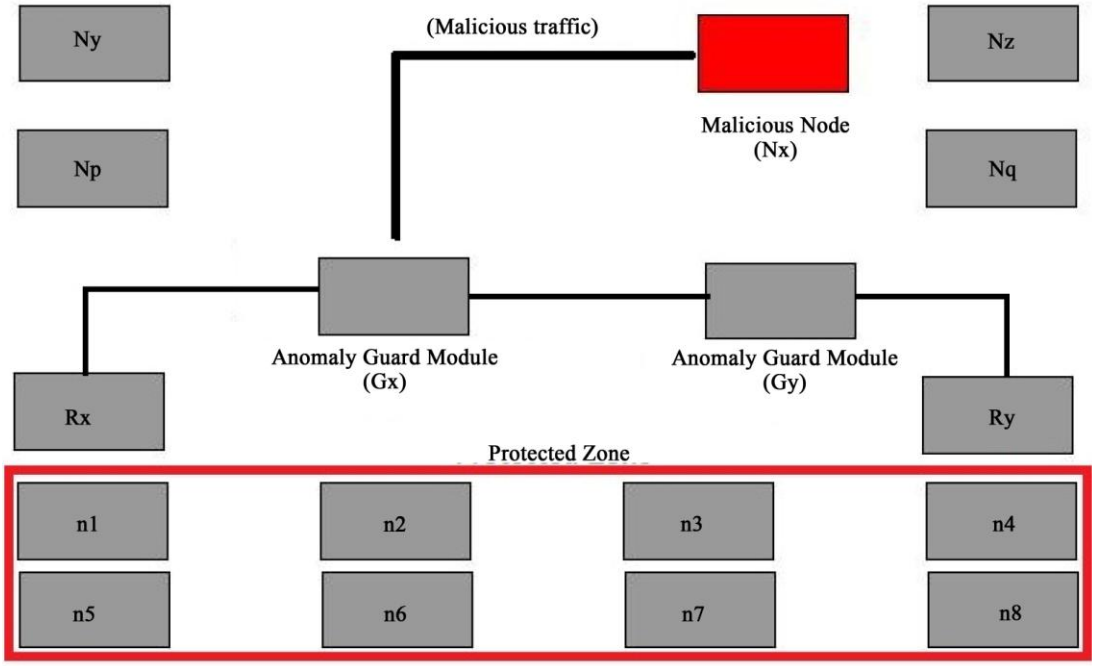

Figure 1. **Illustration of anomaly detection.**

2.2. Anomaly detection systems

In the anomaly detection system, research or research has been carried out in various problem areas, but in the cloud environment they have not been widely studied. Cloud computing anomaly detection technology is still in sight and evolving because it creates problems that have yet to be resolved. Cloud Anomaly Detection Systems detect unwanted traffic on the network, and this can be caused by packet loss, unwanted application behavior, etc.

On a traditional network, the IDS monitor detects and alerts the administrator by deploying IDS at critical points in the user's site. But in a cloud network, IDS must be managed by service providers [6]. The data through which the intrusion occurs is transmitted through the cloud service provider, this allows only the service provider to be the administrator, and the user just needs to depend on the service provider. In most cases, the user is not aware of such actions in order to maintain the reputation and image of the cloud provider. A solution was proposed by Roschke et al. [2]. which integrates and integrates various IDS sensor outputs into a single interface. The communication between the various IDSs follows the Intrusion Detection Messaging Format (IDMEF) standards. Placing IDS sensors at different levels of the cloud, such as the application level, system level and platform level, can improve communication between IDS sensors as well as increase the discovery process in the cloud. The generated routines or warnings are sent to the Event Collector program. The Event Gatherer program acts as a collector of alerts resulting from a cloud intrusion. The notification received by the event collector is converted to the IDMEF standard and stored in the event collector database using a plugin known as the sender and receiver handler plugin [7].

3. Taxonomy of anomalies

Anomaly detection aims to detect the presence of abnormal patterns in network traffic, and the simple detection of such a loop can provide the network administrator with an additional source of information to determine network behavior or track and determine the root cause of network failures [8]. Anomalies can be divided into three categories: point anomalies, context anomalies, and collective anomalies [9] [10].

3.1. Point anomalies

It is when an individual instance of data deviates from its normal activity or shape, it is considered anomalous because the other data is normal. This indicates that the abnormal activity lies outside the normal area. This is the simplest type of anomaly among the three types or categories, and it is the strength or importance of detecting the anomaly. **In fig. 2** shows point anomalies.

From **Fig. 2** , N_1 and N_2 are areas of normal behavior, Points O_1 and O_2 are an anomaly, and Points in an O_3 are an anomaly.

3.2. Context anomalies

Contextual anomalies occur when the appearance of information has or shows traces of an anomalous nature in a precise or precise context, which is the unwanted behavior of actions that surround a single instance of data. **Figure 3** shows a contextual anomaly.

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

3.3. Collective anomaly

This is when the collected associated data instances act as anomalous or exhibit unwanted activity associated with the entire dataset. In a collective anomaly, individual data instances with a collective anomaly are not otherwise called anomalous per se because the collective anomaly requires communication between or between data instances; Sequential, spatial, and graphical data causing a collective anomaly. But their appearance as a whole or in the aggregate is or may be abnormal. **Figure 4** illustrates the Collective Anomaly.

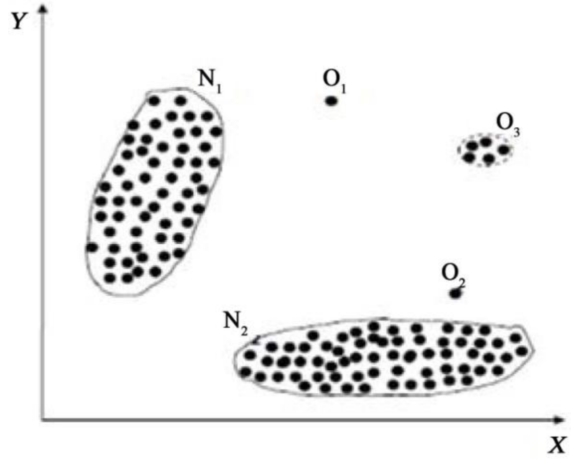

Figure: 2. Illustration of a point anomaly.

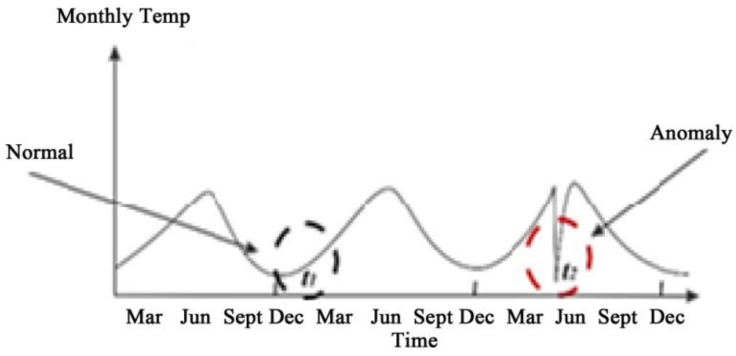

Figure 3. Illustration of a contextual anomaly.

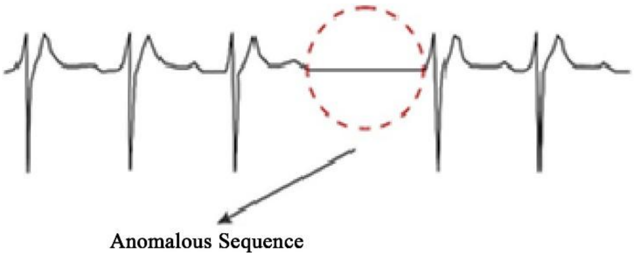

Figure 4. Collective anomaly.

4. Detection of anomalies in cloud networks

In cloud networks, traffic or packet flow comes from more than one domain. The cloud environment is undergoing rapid change due to patterns or behavior of clients / clients using the cloud infrastructure and the state of unsecured services. In the cloud environment, there are various problems associated with anomaly detection, such as misconfiguration or large amounts of legitimate network traffic. The importance of detecting an anomaly in cloud networks is unwanted activity in the data, which leads to the importance of the cause of such an anomaly in the information. Typically, commercial off-the-shelf intrusion detection systems (COTS) are signature-based or rule-based [11] [12].

Signature-based IDS can be used to detect known attacks on the cloud network, although the deployment point can be in front of the cloud to detect external or inbound attacks, or on the inside of the cloud to detect both external and internal attacks.

4.1. Methods and methods for detecting anomalies in cloud networks

In cloud networks, there are various methods or techniques that have been used to detect abnormal activity; these include threshold determination, statistical analysis, rule-based measures, neural networks, genetic algorithms, data mining, and machine learning [13]. This section provides a comparative overview of various methods for detecting anomalies in cloud networks. Comparison between the three main methods or techniques and others will be explored, vise; Statistical analysis, data mining and machine learning.

4.1.1. Statistical anomaly detection systems

This anomaly detection method in the underlying cloud network detects an anomaly by observing the computations in the network and creates a profile that stores or stores the generated value reflecting their behavior. When identifying an anomaly using this method, two profiles are created; the former stores normal or abnormal rules or signatures, while the latter is updated at regular intervals. Anomaly scores are calculated during the update. If the threshold is lower than the currently generated anomaly

profile, then it is known as anomalous and detected. There is a high probability of occurrence of normal data instances in dense areas of the model, while violations are visible in areas of low probability [14]. Some suggested models of statistical anomaly detection
systems: Cloud Diag [15], EbAT (entropy anomaly testing) [16], etc.

The advantages of using this method are that no prior or prior knowledge or training in security risks or subject matter is required. Moreover, it has the ability to detect even recent anomalies generated in the network or data, and there is accurate notification of anomalies that have occurred over a long period of time.

4.1.2. Data Mining Based Anomaly Detection Systems

Analyzing or extracting knowledge from a large dataset into precise patterns useful to the data owner is known as data mining [17] [18]. This method uses classification, clustering and association rule analysis techniques to detect anomalies in the cloud. The analytics engine is a data mining technique that detects anomaly by distinguishing between normal and abnormal activity in the cloud. It does this by establishing or defining some boundaries for what is acceptable and normal in the cloud network. This method also has an extra layer of attention to detect anomalies. Data mining techniques are more flexible and easy to deploy at any time. By integrating data mining into the cloud network, it is possible to extract meaningful information from data warehouses that are integrated into the cloud, thereby reducing infrastructure storage costs. Clients or users of the cloud service should only pay for the data mining tool used [19].

Data mining is commonly used by cloud service providers to provide much better services to their users or customers using their cloud service [19]. The downside to this is that if customers are not informed about the information that was collected and used for mining, their privacy is violated and this is illegal. There are various issues available when mining data mining in cloud networks is a priority substitute for maintaining privacy and setting these privacy settings incorrectly when using different rules and strategies to improve the security of the cloud network.

4.1.3. Anomaly detection systems based on machine learning

The ability of programs or software to improve the performance of its task over time through training is an important method for detecting anomaly. Validated values or normal data behavior are saved when an anomaly occurs or is detected, the machine learns its behavior, saves a new sequence or rule. This method creates a system that can improve the performance of a program by building on previous results. The most interesting thing about this technique is the fact that the improvement in performance from the previous results, the new information is a former prolonged and if it requires a change in strategy execution to improve performance is done on the basis of new information obtained from previous results. There are different categories of anomaly detection based on the tilt of the machine, such as: Bayesian network, genetic algorithm, neural network, etc.

The Bayesian network has the ability to incorporate old knowledge or signatures into its process, as well as anomaly detection data. This method is combined with a statistical mechanism which is very useful in detecting anomalies [20].

Neural networks have the ability to enhance incomplete data to create the potential to detect and understand invisible patterns. The neural network detects not only previous attacks, but also invisible behavior or patterns [21]. Genetic algorithms use evolutionary algorithm methods such as mutation, selection, etc., Their various processes are based on rules gathered from the information of network analysis performed by IDS.

4.1.4. Adaptive AnomalyDetection Systems

Adaptive Anomaly Detection (AAD) systems use hypersphere-based data descriptions for adaptive fault detection. In cloud networks, possible failures or anomalies that are detected by cloud operators are detected by AAD using the performance data of the cloud service. AAD detection systems use or benefit from a log of detected failures that have been submitted by cloud operators to subsequently identify new failure types. The AAD detection algorithm changes its behavior by repeatedly learning new certified results or detections from a cloud provider to be ready for future detections. In accordance with Husanbir C. Pannu et al. [22], a prototype of the AAD system was built and an experiment was carried out to test the prototype in a cloud computing environment with 362 nodes. It was noted that the prototype was lightweight and it took a few seconds for the detector to start up and a few more seconds to set up and detect failures. 518 metrics were profiled every minute, profiling or bypassing all the statistics of a typical cloud server, its CPU usage, task switching processes, memory and paging space usage, paging and page faults, I/O transfers, interrupts, and more. A failure detector such as subspace regularization was used when comparing the ADD algorithm. The failure detector in [23] reaches 67.8% of the sensitivity in experiments. The proposed Bayesian sub models and decision tree classifiers have a detection sensitivity of only 72.5%. In AAD, a failure detector can have detection sensitivity and detection specificity up to 92.1% and 83.8% [22].

As shown in **Figure 5**, it takes 7.26 seconds to detect failures at the middle management node in the cloud network to extract performance metrics, create a hypersphere, and perform failure detection. It is even easier to update the hypersphere and detects glitches in about 2.17 seconds.

5. Comparative overview of cloud security measuresin cloudstorage application.

Cloud storage is a useful way to store data as well as exchange information on the Internet. An important question arises: "Is it safe to store confidential information in the cloud?" well this is the question we are trying toassess

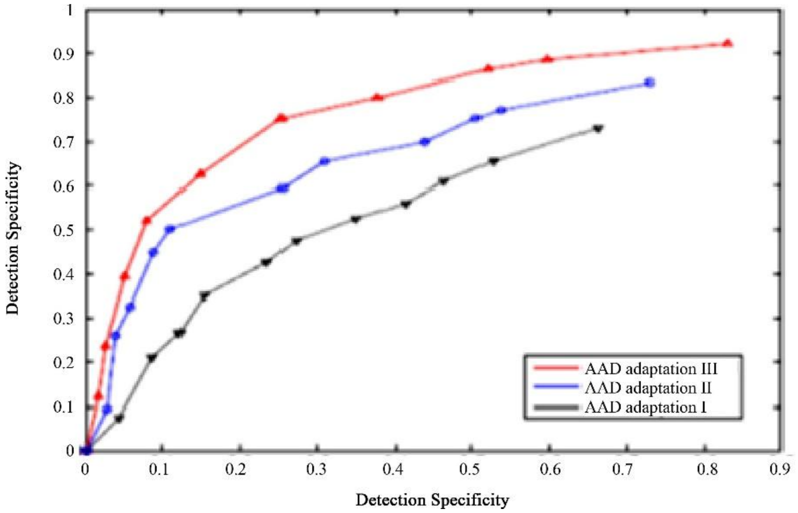

Figure 5. Illustration of failure detection with AAD.

and answer if you can. Cloud security is not a 100% guarantee. Fi e can be encrypted in the transmits of Zion, and at the final destination, the PES can decrypt the file to gain access, because the encryption algorithm used is provided by them. Anyone can access your account and your sensitive files can be compromised. In this case, client-side or user-side encryption is important, and the use of a strong encryption key is recommended.

In cloud computing, computational usability has been moved from the user side to the CSP side; This means that users can access their files from anywhere at any time, even using multiple devices such as laptops, tablets, smartphones, etc., it gives the user a sense of data mobility than just storing data on a computer only at home [20].

5.1. Dropbox

Dropbox is a public cloud storage that was developed by two MIT alumni who always forget or lose their USB devices containing the information they need to use at the moment. This made Dropbox famous in the information technology world. In 2007, the company was founded Dropbox Inc., Which offers cloud storage, client software and file synchronization [21]. Dropbox allows users to upload their files or folders to the Dropbox folder, where they can be viewed or shared on any device at any time as long as Dropbox is installed on the device along with a username and password, and an Internet connection for syncing.

Dropbox was designed for personal use, which was the intent of two MIT alumni, but as of 2011, the cloud application had over 50 million users worldwide with over 20 billion files and petabytes of storage. Dropbox provides 2GB of cloud storage for free, but additional storage can be purchased. The Dropbox app is available for Windows, Apple OS X, Android and Linux [21].

Figure 6 shows an example of how the Dropbox protocol works . The basic mechanism of operation is based on the so-called hand-shake process of the main networking standards.

Dropbox security measures

There are many security issues in the cloud computing environment that affect usability. Dropbox, which is a cloud-based application or storage, has several security measures to ensure the integrity and security of data. Dropbox retains all deleted and earlier versions of files for thirty days; this feature is supported by both free and premium (paid) accounts. A free account only uses the "keep older version of files" feature for 30 days, while a paid or premium account saves files indefinitely. IN

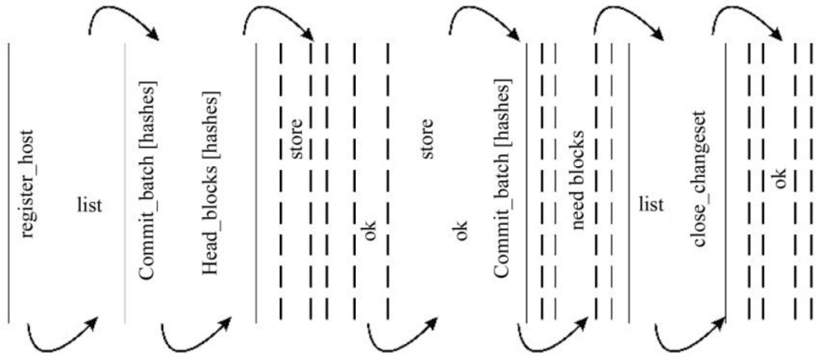

Figure 6. Illustration of the Dropbox protocol.

Amazon S3 (Simple Storage Service) is used in Dropbox cloud computing environment to store files. This is done to ensure high integrity and availability of data, and replication of multiple data centers is used [14].

AES-256 encryption is used to ensure data privacy in the Dropbox cloud environment. In Dropbox, encryption is machine-protected, meaning that the encryption key is stored on the machine and not in the cloud storage [14]. In addition, the Dropbox encryption algorithm uses TEA symmetric encryption [15].

Secure tunnel protocol SSL is used for data transmission and is also the AES-256 encryption standard. A two-step verification process is used to strengthen security controls and is recommended [15] [16]. The availability of third-party applications in the Dropbox cloud also adds another form of encryption security [15] [16]. In addition, Dropbox uses SQLite 3 database to ensure data integrity and non-redundancy in user interactions with the database. All network traffic is transmitted over HTTPS, correct certificate validation is performed during the authentication process, and OpenSSL is used to address security concerns in Dropbox services [17].

Using OpenSSL improves the security of authentication and authorization for Dropbox users. The NCrypt shell is used by Dropbox. The NCrypt wrapper creates security where there is none. NCrypt is an encyptor/decryption file and uses AES as the encryption algorithm [17] [18].

It minimizes the disclosure of the plaintext password in memory and converts the plaintext to a SHA-1 hash before immediately erasing the plaintext from the hard drive, and as soon as SHA-1 is used to generate a key for encryption, it is also erased from memory [17] - [19]. The RSYNC (Remote Synchronization) protocol is used, which allows the user to synchronize files between two or more computer devices, ensuring that the same file is available on all connected devices. Disconnecting a remote device is another technology used by Dropbox [24].

5.2. Google drive

" Google Drive" is a version of Google cloud storage, and it is one of the popular cloud services. It supports photos, videos, documents and other files. 15 GB of free storage is provided, which the user can increase at any time. Google Drive provides generic applications for viewing over 30 file types without having to install the corresponding application on the computer system to view the corresponding file type. Google Drive provides unlimited download rates for uploading files to the appropriate custom drive.

Google Drive security measures

Google Drive is integrated with Gmail services, and once a user becomes the owner of a Gmail account, he can automatically set up a Google Drive account. As Google Drive empl oys a two-step verification feature, data security becomes an important barrier for users of related technologies, as three-tier security architectures are more important and improve data security for users [25] - [27].

In addition, the "cloud lock" feature is used to enhance personal information security and also ensure PCI compliance. Files on Google Drive are encrypted using AES-256 and RSA-4096 standards, and in addition to it, there is automatic encryption of data on Google Drive and server side encryption mechanisms are used [28] [29].

5.3. iCloud

The iCloud - the cloud of Apple’s Inc. It was launched on October 12, 2011 [30]. iCloud offers its users a means for storing data, for example: documents, images, videos, etc. Users can also make backup copies of their devices iOS directly to iCloud over the wireless network. As of July 2013, iCloud had 320 million users [31] [32]. ICloud was first named by I Tools in 2000, Mac in 2002 and MobileMe in 2008 [32].

ICloud security measures

iCloud provides data security of its users by encrypting them when sending via the Internet or at the transition, which also includes a two-step authentication [33]. Protected tokens are used for authentication, this creates secure and unauthorized access both in transit and when stored in iCloud. For messages sent over thenetwork, iCloud introduced iCloud Keychai n, which uses 256-bit AES encryption to store the password as well as store credit card information. It uses asymmetric elliptic curve cryptography and key transfer. Encryption Keys iCloud Keychain is created and stored on the user's device, not on the iCloud server [34] [35]. ICloud sessions are encrypted using SSL to improve the security of your login information, and iCloud uses at least 128-bit AES encryption to encrypt documents. Files to be transferred are encrypted in transit using 128-bit AES encryption [36].

6. Comparison of cloud services: iCloud, Dropbox and GoogleDrive.

The different cloud services outlined in this article have different service requirements for customers as well as their cost. In Table 1, a detailed comparison was made to determine which of the three cloud services has the best security feature. We found that the Dropbox cloud service includes more security measures than Google Drive and iCloud.

Dropbox cloud storage accounts for about 100 GB of traffic every day on one of the monitored networks [37]. To avoid data duplication, a deduplication mechanism has been developed [38] [39]. Dropbox has content sharing capabilities, and the percentage of files or folders shared by home users is around 70%, while connected devices are around 30%. Among students on campus, about 40% use 5 or more folders. Dropbox uses a delta encoding mechanism when uploading or transferring chunks, "a chunk is a split large file." In Dropbox, a file larger than 4MB is split into chunks that are identified by a SHA256 hash value, which is included in the file metadata description [40].

The two main components of the Dropbox architecture that can be distinguished are management and storage [37]. In the Dropbox cloud service, each linked device has a unique identifier (host_int), these unique identifiers are also used for each shared folder in Dropbox. Different devices belonging to the same user are displayed by matching namespace lists [40].

Table 1. Safe comparison of Dropbox, Google Drive and iCloud .

Security measures	Google Drive	Dropbox	iCloud
Secure connection	YES	YES	YES
Encrypting Stored Files	YES	YES	YES
SSL protocol	YES	YES	YES
Open SSL	No	YES	No
128-bit AES encryption algorithm	No	No	YES
Two-step authentication process	YES	YES	YES
HTTPS protocol	YES	YES	YES
Disconnecting a remote device	No	YES	No

AES-256 encryption	No	YES	YES
RSYNC (remote sync)	YES	YES	YES
NCrypt Wrapper	No	YES	No

Content stored in Dropbox can be viewed and accessed using a web interface such as a browser. A different set of domain names are used to identify public and private transactions; URLs containing dl-web.dropbox.com are associated with private content, while dl.dropbox.com is associated with publicly available shared files [37].

Google Drive is best for creating documents and sharing files. You can create spreadsheets, presentations, drawings, new document, and more, and saved files can be accessed anywhere using smartphones with Google Drive apps installed, and desktop apps are available for PC and Mac. Synchronization of files between PC and Google Drive occurs automatically [37].

As shown in Figure 7, Google Drive supports Microsoft Word documents, PowerPoint presentations, Adobe InDesign, Adobe Illustrator, Microsoft Excel, Adobe Photoshop, Wave Audio files, Adobe Reader, and more, with these applications installed on Google Drive via the cloud. service provider, it allows users to easily edit, create and view related documents without having to install the corresponding application on each device.

As Table 1 shows a variety of security measures to Dropbox , the Google Drive and ICloud shows that various different security infrastructure cloud services in the long term data security, availability, and control.

In Table 2 , Dropbox gives 2 GB of free space per subscriber to its cloud services; additional storage space can be added by purchasing the premium package. Google Drive provides its users with 15GB of free storage space, additional storage can also be purchased to increase storage capacity, finally, iCloud provides its users with 5GB of free storage, and additional storage is available to users for a price. For users looking for free high-capacity storage, Google Drive has a better deal. Dropbox, Google Drive and iCloud allow customers to store any type of file on their cloud server. An offline feature is also available so users can download the file to view later even if there is no internet connection.

Dropbox, Google Drive and iCloud allow their customers to store any type of file on their cloud server. Why - A feline feature is also available so that users can download the file for later viewing even if there is no internet connection.

As shown in Table 3, cloud services also vary in price, storage, and performance. Table3 shows the price difference between Dropbox, Google Drive, and iCloud. However, this depends on the user and their choice of product.

Table 4 summarizes the general capabilities of cloud storage applications. As you can see from the table, Dropbox is the only cloud storage app that supports all features, while iCloud and Google Drive do not.

Figure 7. Common Google Drive applications.

Table 2. Comparison of storage between Dropbox, Google Drive and iCloud.

	Dropbox	**Google Drive**	**iCloud**
Storage space	2 GB	15 GB	5 GB
Maximum file space	No data	250 MB	No data
File type	Anything	Anything	Anything
Offline services	YES	YES	YES

Table 3. Cost of service for Dropbox, Google Drive and iCloud.

Storage	Dropbox	Google Drive	iCloud
100 GB	USD 99	60 USD	No data
200 - 250 GB	No data	$ 120 (200 GB)	$ 3.99 (200GB) per month
400-500 GB	$ 499 (500 GB)	$ 240 (400 GB)	$ 9.99 (500GB) per month
1 TB	$ 119.99	USD 600	$ 19.99 / month

2-16 TB	No data	1200-7600 USD	No data

Table 4. Dropbox, Google Drive and iCloud capabilities.

Opportunity	Dropbox	Google Drive	iCloud
Breakdown	YES (4 MB)	YES (8 MB)	No
Equipment	YES	No	No
Client deduplication	YES	No	No
Data encoding	YES	No	YES
Data compression	YES	YES	No

CONCLUSION

Anomaly detection in potentially dangerous networks is an extensive area of research, which contains a large number of developments and proposals for detection systems. Abnormal activities always take place on our networks, both in the cloud and outside of it. Using various types of cloud network anomaly detection techniques or techniques, unwanted behavior detection can be tracked, detected, and stopped. These methods have their limitations that create a gap between their performance metrics. In a cloud network, a hybrid system or anomaly detection method should be used to get a more efficient and high performance system. In this article, we discussed the importance of an anomaly detection system in the cloud, its types, methods and limitations that each method faces, such as generating false alarms; detection accuracy depends on previously collected information about abnormal behavior; it takes more time to detect attacks, etc. These limitations can lead to inaccurate anomaly detection. Extensive research is needed to develop a more robust and efficient model that captures and attempts to improve the limitations of anomaly detection systems. Security in the cloud computing environment is very important as individuals and companies use their services. In this article, we compared the security measures of Dropbox, Google Drive, and iCloud; we found that most cloud service providers have similar security measures, but few are different. Some of their common features are the use of the AES encryption algorithm, communication over HTTPS, the use of SSL, and a two-step authentication process. This helps protect data in transit and in the cloud. Dropbox security measures are generally aimed at protecting the information of cloud users; it includes an Ncrypt shell and a remote device disconnect mechanism. In terms of security, I would say that for a more secure cloud service, Dropbox is the best choice, although you can get more storage with a premium offering, which is expensive but Google Drive is best for storage and variety of apps.

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 6th 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 Pro- gram. 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 12th 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

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

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

35. http://www.whois.net/whois/icloud.de

36. 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

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

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

39. Harnik, D., Pinkas, B. and Shulman-Peleg, A. (2010) Side Channels in Cloud Services: Deduplication in Cloud Storage.

40. IEEE Security and Privacy, 8, 40-47. http://dx.doi.org/10.1109/MSP.2010.187