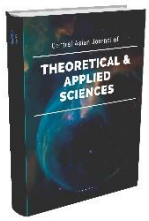


CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 03 Issue: 10 | Oct 2022 ISSN: 2660-5317
https://cajotas.centralasianstudies.org

An Improved Security Solution for Cloud Computing Management Infrastructures: The Insider Perspective

Aburuotu, E. C
School of Post Graduate Studies, Department of Computer Science, Faculty of Natural and Applied Sciences, Ignatius Ajuru University of Education
emmanuel.aburuotu@iaue.edu.ng, emmanuelaburuotu@yahoo.com

Ojekudo, Nathaniel A. (PhD)
Department of Computer Science, Faculty of Natural and Applied Science, Ignatius Ajuru University of Education, Port Harcourt
nathojekudo@gmail.com, nath.ojekudo@iaue.edu.ng

Received 15th Aug 2022, Accepted 16th Sep 2022, Online 19th Oct 2022

Abstract: *This study examines the security of cloud computing management infrastructures from the perspective of the insider attacker. It is also proposed to design and implement a security system for the infrastructures responsible for the management of cloud computing environment against the insider attacker. To achieve this aim, we designed a security solution that handles login verification and login information storage. The application stores the login information of every personnel who has been defined to access the system. The solution also stores information about infrastructure managers, the host server, the virtual server, the smart routers and switches, all of which are used for storage and transmission of data over the internet. The infrastructural security solution is applicable to Infrastructure as a service (IaaS). The system is also capable of handling authentication of cloud members, verification and monitoring of data transfer, thus maintaining network security for our cloud environment and data confidentiality. The security system also provides the administrator with the privilege of monitoring who is logged into the cloud environment, in other to protect the network from hackers. Because design method is required to complete this research, Waterfall Design Methodology was adopted for the research, design and implementation methodology. Programming is performed using PHP, coding is done using HTML platform, Couchbase offline server is used as our local server for hosting this cloud network security system, and advanced network security Standard algorithm is implemented for ensuring security framework.*

1.0 Introduction

The introduction of new technology leads to qualitative growth, but at the same time, there is a high risk of a quantitative data breach. It is important to see the protection of the cloud infrastructure as one of the main obligations when embracing cloud technology. There are different companies out there that are still concerned about the protection of their data in the cloud world. Organizations considering transitioning

their data into the cloud, even those who has already transitioned their data into the cloud are seriously concerned about the security of the data, especially as it concerned Infrastructure as a Service (IaaS). Individuals also are concerned about the security of their data in the cloud. This ranges from business data, analytical data, statistical data, personnel record, financial record etc. Over the years in the research on the security of the cloud management infrastructure, interest and focus has always geared towards the outsider attacker. However, recent researchers have focused on the insider attacker. Many have chosen to leverage on the use of closed-circuit television (CCTV) cameras- Donghyeok et al (2018), many have resorted to using detectives doors, many have chosen to use rack signal alarm raiser, while other organizations have integrated web cameras and time management systems for effective detection, recording, monitoring, evidence collection and decision making. With these efforts and technologies implemented, security of the cloud management infrastructures is still a concern with utmost priority. There is a paradigm shift in the way and method that computing technology and services is administered. Nowadays, a group of connections, applications and resources are accessed over a network with a virtual delegation of task and it is called cloud computing. Collectively, this network of servers and links are known as the cloud. Users have the ability to manage most tasks performed with super-computers by cloud computing. For example, by using a tinny client or other access point, such as an iPhone, BlackBerry or laptop, users can access resources as they need them in the cloud. Cloud computing has also been identified as on-demand computing for this purpose. Cloud computing is very distinct from the conventional model of desktop computing, where it is possible to manage and use resources stored in the database within the same computer.

Due to the benefits of greater flexibility and availability to obtain computing services at lower prices, people have developed an interest in cloud computing in recent years. Network Cloud environment protection and stored resource privacy, however, are a concern for agencies and organizations making the transition to public cloud computing environments with applications and data, which is the impetus behind this research. Government and private sector budgets are declining, according to Todd Steiner; as such,' executives are plotting new tactics to become more competitive and cost-effective- Todd Steiner, (2012). Over the past few years, cloud computing has gained a lot of popularity as a way of reducing IT investment, improving scalability and reducing head-over-head administration. As applicable to a cloud environment (IaaS, PaaS, and SaaS), infrastructural protection consists of the security of the underlying physical environment and the conceptual security controls inherent in the service or available for use as a service -Todd Steiner, (2012). Security of the physical environment ensures sufficient distribution, control, and safety of access to the cloud service through the underlying physical resources within which the service is designed. Logical controls of infrastructural protection consist of services on the connection, protocol, and application layer.

In a cloud environment, a major part of infrastructural security is likely to be provided physically and within the hardware and software running the infrastructure. Tight integration with the underlying cloud software layer to ensure full visibility of all traffic on the virtual network layer is important. In the cloud network, the classic definition of network perimeter takes on different meanings. For many cloud networks, the perimeter is clearly the demarcation point. For other cloud networks, the perimeter transforms into highly dynamic “micro-borders” around individual customer solutions (to the level of certain data sets/flows within a solution) within the same cloud, consisting of virtual network components. In other cloud networks, there is no clear perimeter at all. This causes a challenge within a cloud environment. Typically, the inspection and control of network traffic do not pass through physical interfaces where classical control devices can analyze or block them. This happens when cloud servers use a physical server’s internal memory pipe software switch or even direct APIs). This is another reason why effective controls require the integration with the cloud software layer -Cloud Security Alliance, (2012).

Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This is achieved primarily by leveraging the capacity of a data center. Google and Amazon are two widely known data centers providing Cloud Computing and storage. Software such as VMware has enabled business to create a privately owned Cloud. Along with the gains achieved in Cloud computing there are inherent security risks. For instance, when you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a "cloud computing" service. Cloud computing therefore refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications.

The concept of cloud computing is currently receiving considerable attention, both the research and commercial arenas. While cloud computing concepts are closely related to the general ideas and goals of grid computing, there are some specific characteristics that make cloud computing promising as a standard for transparent, scalable and distributed computing. In particular, two important properties that many cloud systems share are the following:

1. Homogenous Operating Environment: Through virtualization, cloud computing provides a homogenous operating environment. For instance, cloud gives room for identical operating system (OS) and libraries on all cloud nodes.
2. Control Over Dedicated Resources: Cloud computing provides full control over dedicated resources in many cases. The cloud system is set up in such a way that the application has full control over exactly the right amount of dedicated resources, and more dedicated resources may be added as the needs of the application grow.

While these two properties lead to systems that are less general than what is normally considered in the grid computing context, they significantly simplify the technical implementation of cloud computing security solution, possibly to the level where feasible, easily deployable technical solution can be worked out. Indeed, the first property above removes the complexity of dealing with versions of application code that can be executed in a large variety of software operating environments, and the second property removes the complexity of dealing with resource discovery queuing system, reservations, etc which are the characteristics of shared environments with heterogeneous resources. Cloud computing is thus a promising paradigm for transparently scalable distributed computing. The well-known cloud security system is Google's security system and hosting, system. Cloud computing now supports application enterprising. This work is concerned with the infrastructural security of cloud computing and the resources stored in the server-side of the cloud.

2.0 Review of Related Literature

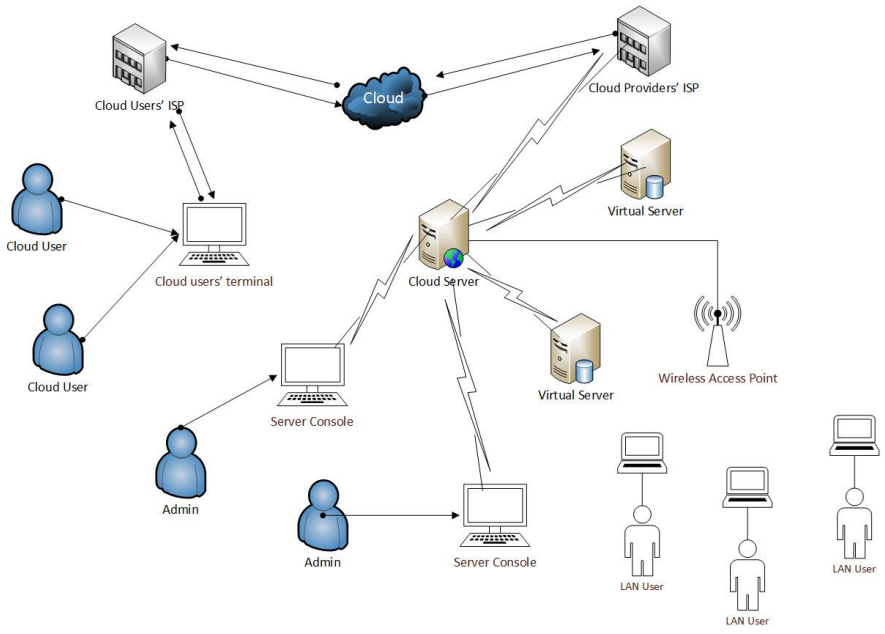
The term cloud computing is rather a concept which is a generalized meaning evolved from distributed and network computing. Cloud computing is described as the offspring of distributed and grid computing by some authors-Monjur Ahmed and Mohammed Ashraf Hossain, (2014).The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done by using someone else's network where ownership of hardware and soft resources are of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially in the form of distributed computing; though this is not apparent or by its definition of cloud computing, do not essentially have to be apparent to the users. In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in

the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier the term ‘cloud computing’ is rather a concept, so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized form of grid and distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion Hashizume et al. (2013). In a pervasive meaning within the context of computer networks, infrastructure could be thought of as the hardware as well as their alignment where platform is the operating system which acts as the platform for the software -Monjur Ahmed and Mohammed Ashraf Hossain (2014)

Thus the concept of cloud based services is hierarchically built from bottom to top in the order of IaaS, PaaS and SaaS. This is merely the level of abstraction that defines the extent to which an end-user could borrow the resources ranging from infrastructure to software – the core concern of security and the fashion of computing are not affected by this level of abstraction. As a result, security is to be considered within any form of cloud computing -Bisong & Rahman, (2011) regardless of flavour, hierarchy and level of abstraction. Virtualization is an inevitable technology that is highly coupled with the concept of cloud computing- Monjur Ahmed and Mohammed Ashraf Hossain, (2014) – it is the virtualization technology that complements cloud services especially in the form of PaaS and SaaS where one physical infrastructure contains services or platforms to deliver a number of cloud users simultaneously. This leads to the addition of total security aspects of virtualization technology on top of the existing security concerns and issues of cloud computing.

Figure 2.1 illustrates typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture

Figure 1. A typical cloud Architecture



Source: (Monjur & Hossain, 2014).

The cloud architecture as illustrated in fig 2.1 is self-explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing concept presented earlier. One notable part from the architecture is that, while the cloud users are clearly identified and named accordingly due to their remote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud service provider's network in the scenario. If the definition of cloud computing is taken to have essential arrangements of being the servers located remotely that are accessed through public infrastructure (or through cloud), then the LAN users in figure 1 may not be considered as the cloud users in the context.

Mehmet et el (2009), proposed a practical security model based on key security considerations by looking at a number of infrastructure aspects of Cloud Computing such as SaaS, Utility, Web, Platform and Managed Services, Service commerce platforms and Internet Integration which was introduced with a concise literature review. The purpose of their research was to offer a macro level solution for identified common infrastructure security requirements. This model with a number of emerged patterns can be applied to infrastructure aspect of Cloud Computing as a proposed shared security approach in system development life cycle focusing on the plan-built-run scope.

Hamid et al (2013) presented a Trusted Cloud Computing Infrastructure approach. Trusted Cloud Computing Infrastructure is proposed inspired by Trusted Cloud Computing Platform. Through presenting a User Trusted Entity (UTE) the proposed approach is supposed to make cloud computing infrastructures reliable in order to enable infrastructure service developers to provide a closed execution environment. One advantage of the proposed UTE is that managers of Infrastructure as a Service (IaaS) systems have no privilege within UTE. Therefore cloud computing managers cannot interfere in Trusted Coordinator functionality. It has been assumed UTE should be kept by a third agent without any incentives to collude with IaaS services and highly trusted to ensure confidential execution of guest virtual machines.

Donghyeok et al (2018) presented that due to the fact that information and communication systems are grafted onto an existing power grid, numerous security risks occur in the smart grid setting. In particular, smart metering data shows a range of information, such as life habits of users and devices in use, and can result in severe breaches of personal information. We are therefore in a situation where there is a need for a de-identification algorithm suitable for metering data. This paper therefore proposes a new method of de-identification for metering results. The approach proposed processes time information and numerical information as de-identification data, respectively, so that the data cannot be analyzed for pattern information. Moreover, such an approach has the advantage that a query such as a direct range search and aggregation processing in a database can be done for statistical processing and usability even in a de-identified state..

2.1 Threats to Cloud Management Infrastructures

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. There are several types of security threats to which cloud computing is vulnerable.

Table 1 provides an overview of the threats for cloud customers categorized according to the confidentiality, integrity and availability (CIA) security model and their relevance to each of the cloud service delivery model.

Table 1: A list of Cloud Security Threats

S/N	Threat	Description
	Confidentiality	
1.	Insider user threats:	Insider user threats: Malicious cloud provider user Malicious cloud customer user Malicious third party user (Supporting either the cloud provider or customer organizations)
2.	External attacker threats:	These includes remote software attack of cloud infrastructure, remote software attack of cloud application, remote hardware attack against the cloud, remote software and hardware attack against cloud user organizations' endpoint software and hardware
3.	Data leakage:	Failure of security access rights across multiple domains and failure of electronic and physical transport systems for cloud data and backups
	Integrity	
4.	Data segregation:	The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated.
5.	User access:	Poor identity and access management procedures
6.	Change management:	Customer penetration testing impacting other cloud customers Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers
7.	Denial of service threat:	➢ Network bandwidth distributed denial of service ➢ Network DNS (denial of service) ➢ Application and data denial of service
8.	Physical disruption:	➢ Disruption of cloud provider IT services through physical access ➢ Disruption of cloud customer IT services through physical access Disruption of third party WAN

		providers Services
9.	Exploiting weak recovery procedures:	Invocation of inadequate disaster recovery or business continuity processes

Source: Sen (2016).

2.4 Types of Attackers in Cloud Computing Infrastructures

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two groups as illustrated in Table 2.

Table 2: A list of attacks on Cloud Computing Environments

1.	**Internal Attackers**	An internal attacker has the following characteristics: ➢ Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service ➢ May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role ➢ Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.
2.	**External Attackers**	An external attacker has the following characteristics: ➢ Has no authorized access to the infrastructure, hardware management data or supporting infrastructure and applications ➢ Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within that enables the management of the infrastructures.

Source: Sen (2014).

Although internal and external attackers of management infrastructures can be clearly differentiated, their capability to execute successful attacks is what differentiates them as a threat to customers and vendors alike.

2.5 Types of Cloud Computing Data Attackers

There are different security issues that occur in cloud computing. These security issues are applicable to both the management infrastructure of any cloud computing model. These security issues are discussed in some of which are discussed below:

2.2.1 Denial of Service (DOS)

When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests. For example a hacker hijacks the web server that could stop the functionality of the web server from providing the services. In cloud computing, hacker attack on the server by sending thousands of

requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack. (Monjur Ahmed and Mohammed Ashraf Hossain, 2014).

2.2.2 Man in the Middle Attack

This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party. Counter measure for this attack is SSL should properly install and it should check before communication with other authorized parties.

2.2.3 Network Sniffing

Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. (Monjur Ahmed and Mohammed Ashraf Hossain, 2014). If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Counter measure for this attack is parties should use encryption methods for securing there data.

2.2.4 Port Scanning

There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks (Services, 2009).

2.2.5 SQL Injection Attack

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an argument value of variable y or 1==1 may cause the return of full table because 1==1is always seems to be true. (Monjur Ahmed and Mohammed Ashraf Hossain, 2014).

2.2.6 Cross Site Scripting

It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials. For example user entered the URL in address bar and attacker redirects the user to hacker site and then he will obtain the sensitive data of the user. Cross site scripting attacks can provide the way to buffer overflows, DOS attacks and inserting spiteful software in to the web browsers for violation of user's credentials. (Monjur Ahmed and Mohammed Ashraf Hossain (2014).

2.2.7 Deletion of Boot Records

Most hardware attackers try to delete the management server book record by attacking the dick structure and Master Book Record (MBBR). Data stored on your hard drive is not only dumped randomly by the machine onto the drive platters. The hard drive of a computer is broken down into separate partitions. In turn, each partition can carry a separate logical drive or an operating system. e.g., if you had one 500 GB drive, it could be split into a C: 250 GB drive and a D: 250 GB drive by disk partitioning software, even though there is only one physical disk. Another operating system, like Linux, could optionally carry the D: drive. The first sector of the drive is the Master Boot Record. It informs the system what the various

partitions are on the physical disk and at what addresses they can be reached. The whole hard drive is made inaccessible if the MBR is removed or corrupted, as the device has no idea where to enter the partitions. Linux overwrites the MBR with a software named GRUB if you install Linux on your machine (for GRand Unified Bootloader). If you plan to uninstall Linux later on, you will need to delete GRUB to restore the MBR. In Microsoft windows server, the boot record is referred to as boot loader.

3.0 Thesis Statement

These notorious data breaches are evidence that consistent security management is needed by storage service providers like Cloud. When we speak about cloud infrastructure protection, several companies falsely believe that their data is well secured and far from cyber criminals' radar. The fact is, by using illegal forms to scan for unsecured databases, these cyber criminals are experts at scrapping exposed vulnerable data. For instance, the term protection for cloud computing infrastructure applies to the entire cloud computing infrastructure that includes a wide variety of policies, applications, and technologies. It also contains controls that are used to secure IP, utilities, applications and data that are virtualized.

3.1 Statement of Objectives

The importance of cloud infrastructure protection is crucial as businesses move their vast volumes of data and infrastructure to the cloud. To provide stability and protection in a network infrastructure, cloud security provides several layers of control. It is a highly essential element in creating a resilient environment that works for companies all over the world to enjoy the advantages of cloud infrastructure security by collaborating with leading private cloud storage security service providers focused on technology to keep the company's security running smoothly. Therefore-

1. This work is proposed to implement a solution for the security of cloud management infrastructures.
2. The solution performs isolation of infrastructure units, paths, authentication, verification and loader of boot records.
3. It monitors stored resources as well as transmitted data, thus maintaining infrastructural security, intelligence and supports the trust and integrity the cloud managers.
4. Programming is performed using JAVA Script and PHP programming language, Couchbase offline was used to host our cloud environment, which scan be accessed using wired and wireless LAN networks, and Advanced Encryption Standard security algorithm is implemented for ensuring security framework.

3.1 Aim and Objectives

The aim of this work is to develop a security solution for the cloud computing management infrastructures from the insider perspective.

The specific objectives are:

1. To design a solution that supports unit isolation of infrastructure as a service for a cloud computing environments;
2. To implement the system using JAVA Scripts, and PHP. The offline hosting platform is provided by Couchbase;
3. To test the system in a real environment.

3.2 Significance of the Study

This work is a referenced architecture that identifies scenarios and application as a security solution for a cloud management infrastructure. It can be used as guidance to those who need and intend to implement a

security solution for the infrastructures that manages the cloud environment. This also applicable despite the cloud model that an organization has adopted for service. This group of persons includes:

- Security professionals, including security officers, security administrators, auditors, and others with responsibility for information technology security
- Information technology program managers concerned with security and privacy measures for cloud computing
- System and network administrators
- Users of public cloud computing services.

This work does not prescribe or recommend any specific cloud computing service, service arrangement, service agreement, service provider, or deployment model. Each organization must perform its own analysis of its needs, and assess, select, engage, and oversee the public cloud services that can best fulfil those needs.

4.0 Research Methodology of System Design

This work adopted a waterfall model for the design and implementation of the proposed system. It was implemented with Java Script (JS) programming language and the user interface (UI) is enabled to run on Hypertext Markup Language (HTML). The Waterfall methodology is a software development life cycle (SDLC) that consists of several consecutive design Phases that follow different sub-processes which flows downwards from the problem definition, analysis, design, coding, testing, implementation and then maintenance. And these phases need to be completed one after the other before moving to the next phase only when it is the preceding phase is completely done. And so, waterfall methodology is recursive in nature, because each phase depends on the other and can endlessly be repeated until it is perfected. Sometimes moving back to the previous stage is necessary due to failure in the current phase. This prevailing model is a principal industry-proven methodology that has resulted in an effective design. This methodology is followed closely in the development of this efficient and improved university integrated data repository system. This model possesses some advantages over other methodologies. These advantages include;

1. The waterfall model is the easiest methodology used in system development since it follows a defined number of steps
2. Using the waterfall model, risk management is reduced unlike the spiral model, risk management with software development.
3. Unlike the spiral model, the waterfall model does not need to reuse any of the phases many times and nit based on the continuous requirement of key components for software development.
4. The development of a prototype is necessary when using a waterfall model.

Waterfall methodology of system development was relevant for this kind of work. Because this research focus was to identify the most relevant security issues associated with the management infrastructures that supports the operations and activities of the in cloud computing environment, there was a need to handle the solution development stage by stage until the task is completed.

5.0 Discussion and Results

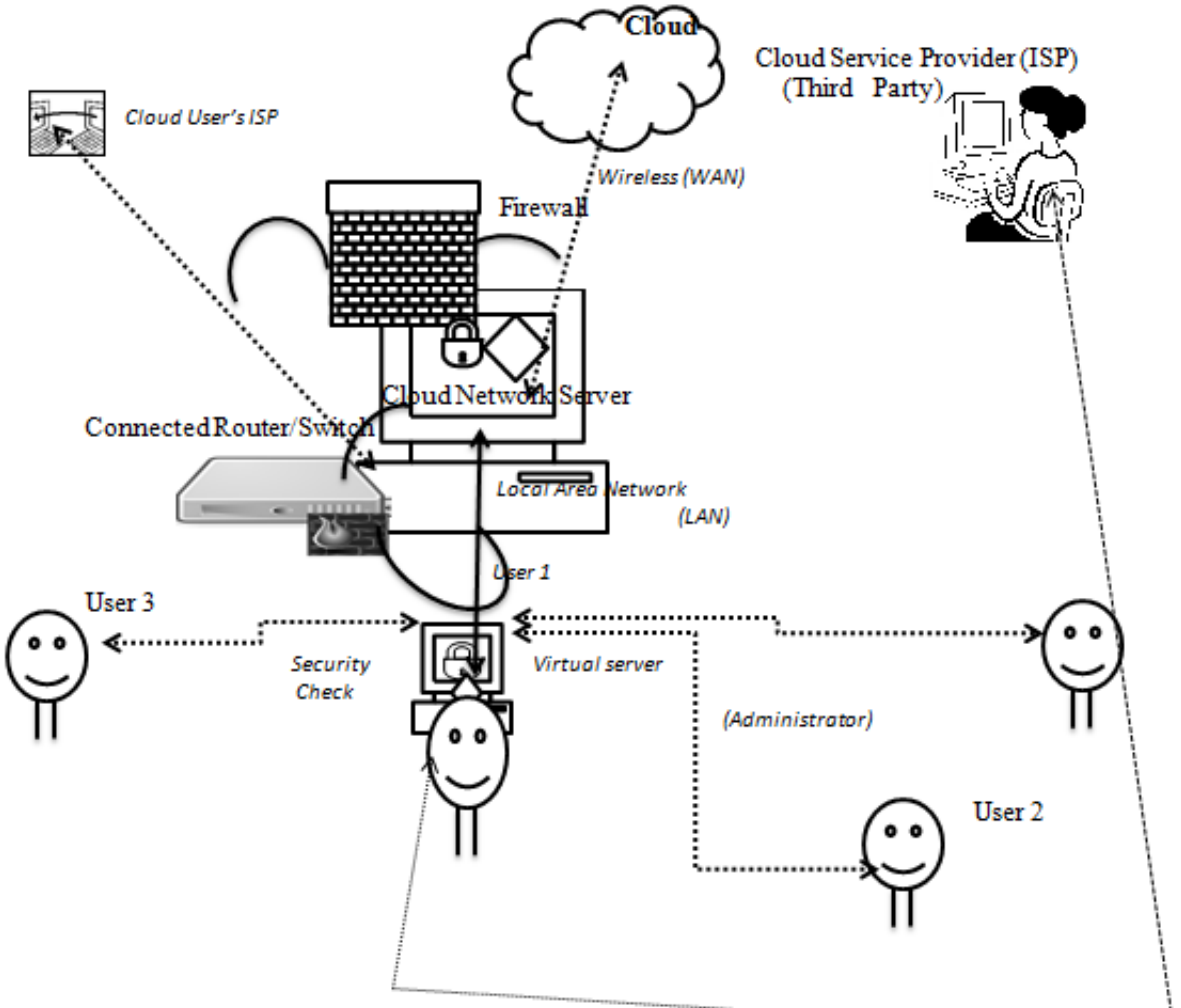
Hardware Units Isolation and Separation of Boot Records

In the proposed system, the security solution for our management infrastructure is developed with the capability of handling isolation of infrastructure storage units and security of boot loader. It can also

handle authentication of users from the index page which is built with a two-way security mechanism. We designed and implemented an authentication webpage with the mechanism of authenticating hardware managers and enable them access to the management infrastructure domain. The administrator has the privilege to access, update, delete, monitor and modify every platform and to manage the resources on the cloud network. However, clients have access to their hardware units and the platform they manage, but are restricted to other platforms owned and managed by others. Our cloud pages contain different resources which parts were used for this research work.

The proposed system is also built with a web application firewall (WAF) and intrusion detection system (IDF) mechanisms, which serves as a server plugin or filter that applies a set of rules to an HTTP conversation to detect many attacks and block them. The virtual machine handles authentication, monitoring and transfer of data over the network when the network server responds to its request.

The Architecture of the proposed system is illustrated in Fig 5.0



5.0: Architecture of the Proposed Cloud computing management infrastructure security solution

The architecture in Figure 5.0 presents a security solution for the infrastructure as a service on the cloud computing platform. It ensures that administrators are not allowed to access or login to the unit and

domain they are not allowed to. This no doubt protects our infrastructure and its services. System for our cloud computing environment. The different function of the security mechanisms:

1. **Hardware Unit Isolation**

The separation of the storage units in a management server is paramount in the security of the management infrastructure of the cloud computing environment. Therefore the proposed hardware section was the storage section of the server machine. The storage units are separated into two different units without partition. As such management console applications are installed in a section from the data.

2. **Protection of Boot Records:**

When providing a security solution for the management infrastructure in the cloud environment, another consideration is to provide high levels of network isolation between all of the different networks within the environment. These infrastructures include management networks, cloud/virtual server, IP storage networks, and individual customer networks; which may in turn be further broken down into segregated networks such as databases, file servers, virtual desktops etc. However, boot records of the infrastructures should be protected from third party operators as such, the management systems can load the operating programmes and the security applications this work proposed.

5.1 Strong Authentication, Authorization, and Auditing Mechanisms

It is very important in any shared environment to ensure that users and administrators of the system are properly and securely authenticated, are only able to access the resources they need to do their jobs or the resources that they own within the system, and nothing more. It also is very important in cloud to know who is doing what within the system, and when their actions occurred. The needs to provide separation of duties and enforce least privilege apply to both the cloud environment and the customer. The cloud owned organization should ensure that its administrators have access only to what they need and nothing more. They also should provide the customer with a mechanism to ensure that the customer's own administrative staff has required access to needed resources. Any access to cloud resources by either the customer or the cloud provider should be logged for auditing purposes. A key part of any ability to audit across multiple systems is a method to consolidate and analyze the logs and monitoring data relating to those systems. Best practice for multicomponent audit systems is the installation of a Security Information and Event Monitor (SIEM) which is implemented as a part of the new system.

5.1 Advantages of the Proposed System

- It is managed by an administrator and not a group of users.
- It is a secured infrastructure security system for a cloud computing environment.
- It handles authentication, thereby protecting out cloud network, no matter their locations
- The system is designed against both external and internal workforce.
- System handles multi-user access
- It is restricted against any who is not a member of this platform. It therefore eliminates the stress involved in the traditional cloud computing system that is one way cloud computing, where anyone can penetrate the platform including the cloud provider.
- Stored files can be accessed from anywhere via Internet connection, hence this requires security investigation.
- Encourages team work

5.2. Disadvantages of the Proposed System

- Requires the services of efficient and professional hardware personnel
- Requires mirror image (sub-server) to mitigate failure on the server
- Requires constant monitoring of the hardware against fail-over
- Requires high capital cost for infrastructure procurement and management
- Requires internet connection for all processes**.**
- It is expensive to maintain this kind of platform.

6.0 Conclusion

For many individuals and organizations, cloud computing is the storage option. While Cloud services offer flexibility, scalability and economies of scale, there have been commensurate concerns about the security of management infrastructures. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own cloud and migrating to Cloud services. Cloud services such as Software as a service, Platform as a service or Infrastructure as a service have their own security concerns which have been addressed in this work. It is also noted that cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store, use and transmit your information or use its applications. Doing so may give rise to certain privacy implications, which security issues were captured and handled in this work. Attention was given more to the security of the cloud management infrastructures which is referred to as Infrastructure as a Service (IaaS).

References

1. Amara Naseer Huang Zhiqui Awais Ali (2017). *Cloud Computing Security Threats and Attacks with Their Mitigation Techniques*. Conference: 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (Cyber).
2. Antonio Celesti; Francesco Tusa; Massimo Villari; Antonio Puliafito (2010). Security and Cloud Computing: InterCloud Identity Management Infrastructure. Published in: 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises.
3. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). *Draft: cloud computing synopsis and recommendations.* National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf
4. Bertion, E., Paci, F., & Ferrini, R. (2009). *Privacy-preserving digital identity management for cloud computing*. IEEE Computer Society Data Engineering Bulletin, 1-4.
5. Bruening, P. J., & Treacy, B. C. (2009). *Cloud computing: privacy, security challenges.* Bureau of National Affairs.
6. Brunette, G. (2009). Cloud security alliance: *security guidance for critical areas of focus in cloud computing.* https://cloudsecurityalliance.org/csaguide.pdf
7. Enoch, N. O. (2012). *Information systems development- a structured approach.* Oyas Bee Enterprises.

8. European Network and Information Security Agency (ENISA) (2009). *Cloud computing: cloud computing: benefits, risks and recommendations for information security*. European Telecommunication Standards Institute. http://www.etsi.org

9. Kannan, M., Lee, S., Solsky O., & Smith, J. (2009). Centre for the protection of natural infrastructure (CPNI)'s information security briefing on cloud computing. http://www.cpni.gov.uk/Documents/Publications/2010/2010007

10. Kean, R., Harris, D., & Meegan, J. (2012). *Security for cloud computing, 10 steps to ensure success.* Clouds Standards Customers Council. http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf.

11. Ko, M., Ahn, G.-J., & Shehab, M. (2009). *Privacy-enhanced user-centric identity management*. In Proceedings of IEEE International Conference on Communications. Pp.998-1002.

12. Mell, P., & Grance, T. (2009). *The NIST definition of cloud computing*. National Institute of Standards and Technology. (www.csrc.nist.gov).

13. Mell, P., Grance, T. (2010). The NIST definition of cloud computing. *Communication. ACM, 53*(6), 50-61.

14. Monjur, A., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of the Network Security and Its Applications, 6*(1), 64-77. http://airccse.org/journal/nsa/6114nsa03.pdf.

15. Mehmet Yildiz; Jemal Abawajy; Tuncay Ercan; Andrew Bernoth (2009). A Layered Security Approach for Cloud Computing Infrastructure. 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. DOI: 10.1109/I-SPAN.2009.157.

16. Naseer, A., Zhiqui, H., & Ali, A. (2017). *Cloud computing security threats and attacks with their mitigation techniques.* International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (Cyber). http://www.doi.10.1109/CyberC.2017.37

17. Qaisar, S., & Khawaja, K. F. (2012). Cloud computing: network/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 34-50. www.journal-archives.webs.com/1323-1329.pdf.

18. Sen, J. (2012). *Security and privacy issues in cloud computing.* Innovation labs, Tata consultancy services. http://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf.