First International Conference on Computer Engineering
International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
Volume 5 Issue 8, November-December-2020

Holistic Empirical Study on Cloud Computing Ecosystem Security Issues

Peter S. Nyakomitta[1*], Silvance O. Abeka[2], Kwach Johnson Kisera[3]
[1*]Faculty of Biological and Physical Sciences, Tom Mboya University College, P.O. Box 199-40300, Homa Bay, Kenya
[2]Department of School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya
[3]Faculty of Biological and Physical Sciences, Tom Mboya University College, P.O. Box 199-40300, Homa Bay, Kenya

ABSTRACT

The advent of cloud computing technology offers gorgeous and innovative computing services through resource pooling and virtualization techniques. Cloud providers deliver various types of computing services through the deployment delivery models to customers according to a pay-per-use economic model. However, this technology shift introduces a new concern for enterprises and businesses regarding their data security issues. The paper intends to provide holistic empirically study of cloud computing ecosystem security issues focusing on the current state-of-the-art of cloud computing delivery, deployment models, cloud virtulization technology and network component. The study deployed systematic empirical study approach that was used to review the most profound literature on cloud computing ecosystem in-line with security issues prompted by the fact that service provider necessarily has access to all the data on the cloud and can accidentally or deliberately disclose it or use it for unauthorized purposes. These findings can be used to understand the potential security issues on cloud computing ecosystem hence the study proposed a model with security components to be embedded in cloud based system. It includes authentication and authorization mechanism as a check for the identity of both cloud subscribers and providers.

Keywords : Cloud Computing Ecosystem , Virtualization, Network Isuue, Service Model, Deployment Model

I. INTRODUCTION

Cloud computing technology is a new paradigm that offers the next generation with internet-based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing technology was introduced by [1] under NIST as "*a technology for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*". The two main key characteristics of cloud computing models are Multi-tenancy and elasticity. Multi-Tenancy enables sharing the same service instance among different tenants while elasticity is the ability to right-size resources as they are needed. It allows optimization of system and captures all transactions. Fiqure 1, depicts cloud computing ecosystem as discussed in the sub-sections below.

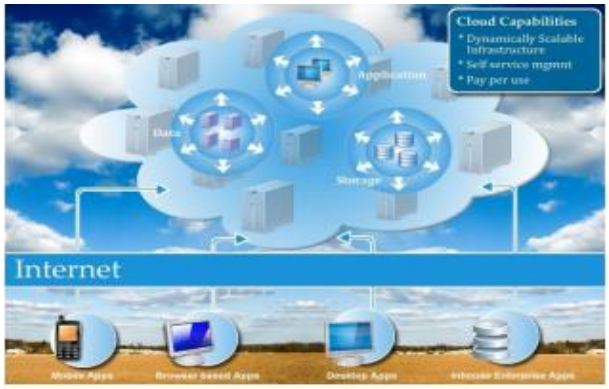

Figure 1 : Conceptual view of cloud computing

Some of the services delivered in cloud computing includes: applications, support services, mail-filtering services, storage services etc as indicated in fiqure 1. The cloud model has motivated industry and academia to adopt cloud computing to host a wide spectrum of applications ranging from high computationally intensive applications down to light weight services [2]. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major hindrance as indicated by [3] in slowing down its adoption, infact ranked first as the greatest challenge issue of cloud computing as depicted in figure 2.

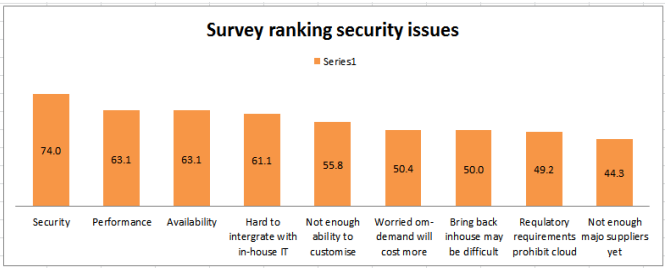

Figure 2 : IDC survey ranking security issues, 2008

From one point of view, security could improve due to centralization of data and increased security-focused resources. According to [4], assessing the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. The current acceptance of cloud computing is linked with various challenges because users are still skeptical about its authenticity. The cloud act as a big black box, nothing inside the cloud is visible to the clients and clients have no idea or control over what happens inside a cloud even if the cloud provider is honest, its only malicious system admins who can tamper with virtual machines and violate confidentiality and integrity.[5]. In this paper, we conducted holistic empirical study on cloud computing ecosystem security issues that has emanated in the cloud environment, laying emphasis on service delivery model, deployment model and the network section.

II. Research Objectives

The objective of the study was to carry out an holistic empirical review of the security issues in cloud computing ecosystem specifically on delivery model, service model, other technologies like virtulization and network and propose a security model that can be used to eliminate ilicit access to the cloud.

CURRENT STATE-OF-THE-ART OF CLOUD COMPUTING ECOSYSTEM

The sub-section presents the review of cloud computing issues in regards to cloud computing deployment model, delivery service, network issues and vitualization technology.

2.1. Deployment Models and its security issues:

Based on the requirements and the services provided by the companies to the subscribers, cloud computing can be deployed in an organization through several deployment models. The sub-section below details the most common types of cloud deployments with their security limitations.

2.1.1. Private cloud.

Private cloud model is generally deployed within an organization and is limited only for the internal access by individuals of that organization. Sub-section below details some specific security issues towards this private cloud model.

Elastic Perimeter- A cloud infrastructure, particularly comprising of private cloud, creates an elastic perimeter. Various departments and users throughout the organization allow sharing of different resources to increase facility of access but unfortunately lead to data breach problem. Moreover,[6] states that elasticity of various cloud based resources would lead to store replicated data on untrusted hosts and this would then lead to enormous risks to data privacy.

Security Control:- The organizations those who are using private cloud infrastructure should need to ensure that effective control of the new environment. [7] stated that the private cloud management architecture should enable management to view security aspects of the environment and show the current threat levels to the organization. The control oversight is to be provided through a web based dashboard that translates the security issues into understandable languages.

2.1.2. Public cloud

Public cloud model is employed by the organization for gaining access to various resources, web applications, and services over any of internet, intranet as well as extranet. Public clouds providers are large targets for hackers. Sub-section below represents security issues related to public cloud model.

Cloning and Resource Pooling:- Cloning deals with replicating or duplicating of the data. According to [8], cloning leads to data leakage problems revealing the machine's authenticity. While [9] describes resource pooling as a service provided to the users by the provider to use various resources and share the same according to their application demand. Resource Pooling relates to the unauthorized access due to sharing through the same network. While the study on Virtual and Cloud Computing by various researches states that a virtual machine can easily be provisioned, they can also be inversed to previous cases, paused, easily restarted, readily cloned and migrated between two physical servers, leading to non-auditable security threats Motility.

Motility of Data and Data residuals:- For the best use of resources, data often is moved to cloud infrastructure. As a result the enterprise would be devoid of the location where data is put on the cloud. This is true with public cloud. With this data movement, the residuals of data is left behind which may be accessed by unauthorized users. According to [10] data-remnant causes very less security threats in private cloud but severe security issues may evolve in public cloud donations. This again may lead to data security threats like data leakage, data remnants and inconsistent data, as stated by [11]. The authors have also mentioned that in order to solve the problems with data storage the optimal solution of cryptography can be thought of effectively.

Shared Multi-tenant Environment:- Multi-tenancy is one of the very vital attribute of cloud computing, which allows multiple users to run their distinct applications concurrently on the same physical infrastructure hiding user data from each other [12]. But the shared multi-tenant character of public cloud adds security risks such as illegal access of data by other renter using the same hardware. A multi-tenant environment might also depict some resource contention issues when any tenant consumes some unequal amount of resources. This might be either

due to genuine periodic requirements or any hack attack [13], has shown that multi-tenancy makes the impact of VM Hopping attack potentially larger than conventional IT environment.

2.1.3. Hybrid clouds.

Hybrid cloud is the combination of two or more clouds (public and/or private). It is an environment providing multiple service suppliers, both internal and external. A hybrid cloud can be considered an intermediate stage as it capitalizes on the benefits of both public and private cloud. But hybrid cloud isn't perfect; it still includes a few security obstacles [14] . The sub-section below discusses some of the security limitations to hybrid cloud.

Lack of Encryption:- Data encryption is a process that helps to address various external and malicious threats. Unencrypted data is vulnerable for susceptible data, as it does not provide any security mechanism. These unencrypted data can easily be accessed by unauthorized users. According to [15], unencrypted data risks the user data leading cloud server to escape various data information to unauthorized users. These unencrypted, insecure data, as per [16], incite the malicious users to misuse the data one or the other way.

Absence of data redundancy:- Problems are inevitable for any cloud providers even though they took best efforts. Hybrid cloud is a complex system. That management has limited experience in managing and that creates great risk. Cloud architects need redundancy across data centers to moderate the impact of an outage in a single data center. A lack of redundancy can become a serious security risk in hybrid cloud, specifically if redundant copies of data are not distributed across data centers. It's easier to move virtual machine (VM) instances between data centers than between large data sets.

Compliance:-In a hybrid cloud maintaining and demonstrating compliance is more difficult. Not only you have to ensure that your public cloud provider and private cloud are in compliance, but also must demonstrate that the means of coordination between the two clouds is compliant. For example if your company works with payment card data, you may be able to demonstrate that both your internal systems and your cloud provider are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

Risk management:- Information security is very difficult to manage risk from a business perspective. Cloud computing (hybrid cloud in particular) uses new application programming interfaces (APIs), requires complex network configurations, and pushes the limits of traditional system administrators' knowledge and abilities.These factors introduce new types of threats.

2.2. Delivery Service models and its security issues.

According to [17], in "The NIST Definition of Cloud Computing," Special Publication 800–145, NIST, broadly divides cloud delivery services into three service models as described in the sub-section below:

2.2.1. Software as a Service (SaaS):

A service is classified as a software if it allows the end user to access and use a provider software application that is hosted, deployed, and managed by the provider from various devices through a thin client interface such as web browser. The users normally have limited control over the application, and are restricted in how they can use and interact with the application. The burden of the security lies with the cloud provider. In part, this is because of the degree of integrated

functionality with minimal user control or extensibility. Sub-section below discusses the various security issues with SaaS.

Application security- SaaS applications are typically delivered via the Internet through a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS aplications. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data [18]. Security challenges in SaaS applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary [19].

Multi-tenancy- According to [20], SaaS applications can be grouped into maturity models that are determined by the characteristics such as: scalability, configurability via metadata, and multi-tenancy. In the first maturity model, each customer has his own customized instance of the software. This model has drawbacks since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high.

Data security:- Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security. In SaaS, organizational data is often processed in plaintext and stored in the cloud [21] states that the SaaS provider is the one responsible for the security of the data while is being processed and stored, also data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well [22]. Cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation and security that must be enforced by the provider.

Accessibility:- Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The [23] has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

2.2.2. Platform-as-a-Service. (PaaS)

PaaS is a moder in which a layer of software or development environment is encapsulated and offered as aservice, upon which other higher levels of services are built. The cloud user has the freedom to build his own applications, which run on the providers infrastructure. PaaS application security comprises two software layers: According [24], security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. PaaS data security issues are described as follows:

SOA related security issues – the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks [25]. Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services. This

security issue is a shared responsibility among cloud providers, service providers and consumers.

API Security - PaaS may offer APIs that deliver management functions such as business functions, security functions, application management etc. Such APIs should be provided with security controls and standards implemented, such as [29]. to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

Third-party relationships:- PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups [27]. Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security [28]. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services.

Underlying infrastructure security:- In PaaS, developers do not usually have access to the underlying layers, so providers are responsible for securing the underlying infrastructure as well as the applications services [29]. Even when developers are in control of the security of their applications, they do not have the assurance that the development environment tools provided by a PaaS provider are secure.

2.2.3. Infrastructure-as-a-Service. (IaaS)

It's a model that provides infrastructure components to clients on demand. The infrastructure components include virtual machines, storage, networks, firewalls and so. With the Iaas, clients have direct access to the lowest-level software in the stack that is operating system which are exposed to some cloud security risk. Sub-section below presents the security issues with IaaS.

Data Leakage Protection and Usage Monitoring:- Data stored in IaaS infrastructure in both private and public cloud needs to be monitored closely [30]. This is essential when IaaS is deployed in public cloud. In this, it should be known that who is accessing the information, how it is accessed, location from where it is accessed and what happened to accessed information later. These problems can be solved by using modern Rights Management services applying restriction to business critical data. Policies for information need to be created and deployed. In addition, transparent process can be created that monitors information usage.

End to End Logging and Reporting:- The effective deployment of IaaS demands comprehensive logging and reporting in place. Robust logging and reporting solutions helps to keep track of where the information is, who accesses it, which machines are handling it and which storage arrays are responsible for it. These solutions are important for service management and optimization.

Authentication and Authorization:- Robust authentication and authorization helps to get effective Data Loss Prevention (DLP) solution. For every application, just user name and password is not most secure authentication mechanism. Sometime two factor or multi-factor authentication is needed [31]. We need to consider tiering access policies based on level of trust.

Infrastructure Hardening:- "Golden-image" VM and VM templates need to be hardened and cleaned [32]. This can be done while images are created. On

regular basis, testing of these master images need to be done.

End to end encryption:- IaaS as a service, both in public and private clouds, needs to take advantage of encryption from end-to-end. We can make use of whole disk encryption to encrypt all the data including user files on the disk. This prevents offline attacks. In addition to disk encryption, all communications to host OS and VMs in the IaaS infrastructure are encrypted. This can be done over SSL/TLS or IPSec.

2.3. Network issues on Cloud:

Network components are shared by different ternants due to resource pooling. Sharing resources allows attackers to launch across-tenant attacks [33]. The virtual networks increase the VMs interconnectivity, an important security challenge in cloud computing. The network is used to upload all the information. With the same aspect, [34] have stated security issues with network on cloud as a prime focus. It provides virtual resources, high bandwidth and software to the consumers on demand. But in reality, the network structure of this cloud faces various attacks and security issues like:

Browser Security:- Every client uses browser to send the information on network. The browser uses SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host. [35]. states that in order to overcome this, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally. Moreover, [36], has shown that Web Services security (WS-security) concept on browsers work with XML encrypted messages which does not need to be decrypted at intermediated hosts.

SQL Injection Attack- These attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information. Further, SQL injection attacks as described by [37] uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker is misread by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to easily access and modify the functioning of a website. [38] have discussed in their paper on how the network related issues hinder the cloud computing and have also shown the SQL injection attack as the top intrusion detection.

Flooding Attacks- In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests. As per the study carried out by [39]. flooding attack consume the critical system resources in order to paralyze the provided services and make them unavailable to its legitimate users in the cloud ecosystem.

XML Signature Element Wrapping:- It is found to be a very renowned web service attack. According to [40], it protects identity value and host name from illegal party but cannot protect the position in the documents. The attacker simply targets the host computer by sending the SOAP messages and putting any scrambled data which the user of the host computer cannot understand. As per the studies carried out by researchers at Ruhr University, and mentioned by the editor [41], the XML Signature wrapping attack changes simply the content of the signed part of a message without tampering the

signature. This would not let the user to understand the twisted data, thus misguiding and misleading the user.

Incomplete Data Deletion:- Incomplete data deletion is treated as hazardous one in cloud computing. According to [42], when data is deleted, it does not remove the replicated data placed on a dedicated backup server. The operating system of that server will not delete data unless it is specifically commanded by network service provider. Precise data deletion is majorly impossible because copies of data are saved in replica but are not available for usage.

Locks in- Another issue is locks in; at this time there is a small tender in the manner of tools, standard data format or procedures, services edge that could undertake data, application and service portability. This will not enable the customer to shift from one cloud provider to another or shift the services back to home IT location [43].

2.4. Virtualization: It has been the underlying concept towards such a huge rise of cloud computing in the modern era. It allows the cloud users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications [44]. However, it also introduces new opportunities for attackers because of the extra layer that must be secured. Virtualized environments are vulnerable to all types of attacks for normal infrastructure and [45] stated that that security is agreater challenge as virtualization adds more points of entry and more interconnection complexity. The sub-section discusses the security weakness in cloud virtualization technology.

Securing VM images repository: Unlike physical servers, VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that such templates may retain the original owner information which may be used by a new consumer.

VM Hopping:- [46] and [47], stated that, with VM hopping, an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM's resource procedure, alter its configurations and can even delete stored data ,thus putting it in danger the VM's confidentiality, integrity and availability. With multi-tenancy, it makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures.

Hypervisor security:- A hypervisor is responsible for virtual machines isolation; therefore , if the hypervisor is compromised, its virtual machines may potentially be compromised as well. The hypervisor is alow-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws [48]. Hypervisor security is the responsibility of cloud providers and the service provider. In this case, the SP is the company that delivers the hypervisor software such as VMware or Xen.

Side channel attacks:- An emerging concern for cloud delivery models using virtualization platforms is the risk of side channel attacks causing data leakage across co-resident virtual machine instances. However, it is possible that attackers who fail to compromise endpoints or penetrate cloud

infrastructure from outside the cloud perimeter, may consider this technique - acting as a rogue customer within a shared cloud infrastructure to access other customers' data.

CLOUD COMPUTING TAXONOMY CLASSIFICATION

The aim of this paper is to conduct holistic empirical study on cloud computing security in order to gain in-depth understanding of their security issues as far as the service is concerned. Figure 3, details the security issues reviewed in each and every model within the cloud computing ecosystem.

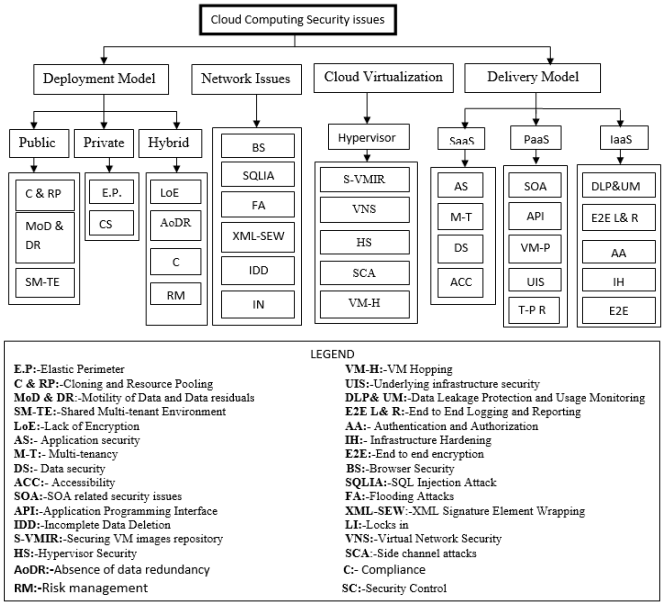

Figure 3. Security Taxonomy tree of cloud computing security issues

III. RELATED WORKS

Various security issues across cloud computing ecosystem as been reviewd by virous researchers on both the cloud provider and cloud user sides. The security responsivities of cloud providers include integrating solutions to ensure legitimate delivery of cloud services to cloud consumers. The security propositions that are necessary for the activities of cloud providers as reviewed in sub-section below.

Authentication and Authorization:- In his article [49] proposed a credential classification and framework for analyzing and developing solutions for credential management that include startegies to evaluate the complexity of cloud ecosystems. This study identifies a set of categories relevant for authentication and authorization for the cloud focusing on infrastructural organization and adapt these categories to the cloud context. In other work relevant with this security factor, a design model for multi-factor authentication in cloud computing environment is proposed [50] for analysis of the potential security threats. Another authentication solution is seen with MiLAMob [51], which provides a SaaS authentication middleware for mobile consumers of IaaS cloud applications. MiLAMob is a middleware-layer that handles the real-time authentication events on behalf of consumer devices with minimal HTTP traffic. FermiCloud [52] uses another approach for authentication and authorization - it utilizes public key infrastructure (PKI) X.509 certificates for user identification and authentication. Authorization-as-a-service (AaaS) approach using a formalized multi-tenancy authorization system, and providing administrative control over enhanced fine-grained trust models was introduced by [53]. They further propose use of cryptographic RBAC to enforce authorization policies regarding the trustworthiness of roles that are evaluated by the data owner.

Identity and Access Management:- The important functionalities of identity management systems for the success of clouds in relation to consumer satisfaction is discussed in [54]. He further presented an authorization system for cloud federation using Shibboleth - an open source implementation of the

security assertion markup language (SAML) for single sign-on with different cloud providers. This solution demonstrates how organizations can outsource authentication and authorization to thirdparty clouds using an identity management system. [55] also propose an integral federated identity management for cloud computing.

Confidentiality, Integrity, and Availability:- Both [56, 57] proposed a design that enables users to verify the integrity of VMs in the cloud. The proposed solution is called the trusted cloud computing platform (TCCP). In this approach, all nodes run a trusted virtual machine monitor to isolate and protect virtual machines. A TCCP guarantees confidentiality and integrity in data and computation and it also enables users to attest to the cloud service provider to ensure whether the services are secure prior to setting up their VMs. In 2011, [58] proposed CloudProof as a secure storage system to guarantee confidentiality, integrity and write-serializability using verifiable proofs of violation by external third parties. Confidentiality is ensured by private keys that are known only to the owner of the data that is to be encrypted. The main idea behind CloudProof is the use of the attestation mechanism. Attestations provide proof of sanity of users, data owners and cloud service providers. The attestation structure implements a solution called “block hash” for performing integrity checks through signature verification.

Fuzzy authorization (FA) for cloud storage [59] is another flexible and scalable approach to enable data to be shared securely among cloud participants. FA ensures confidentiality, integrity and secure access control by utilizing secret sharing schemes for users with smartphones who are using the cloud services. [60] improve cloud service resilience using a load-balancing mechanism called brownout. The idea behind this solution is to maximize the optional contents to provide a solution that is resilient to volatility in terms of flash crowds and capacity shortages (through loadbalancing over replicas) when compared to other approaches that are implemented using response-time or queue length. In another effort [61] the authors proposed a synchronization mechanism for cloud accounting systems that are distributed. The run time resource usage generated from different clusters is synchronized to maintain a single cloud-wide view of the data so that a single bill can be created. The authors also proposed a set of accounting system requirements and an evaluation method which verifies that the solution fulfills these requirements.

Security Monitoring and Incident Response:- According to [62] presents a centralized monitoring solution for cloud applications consisting of monitoring the server, monitors, agents, configuration files and notification components. Redundancy, automatic healing, and multi-level notifications are other benefits of the proposed solution which are designed to avoid the typical drawbacks of a centralized monitoring system, such as limited scalability, low performance and single point of failure. A scalable distributed monitoring system for clouds using a distributed management tree that covers all the protocol-specific parameters for data collection was presented by [63]. Hypervisor-based cloud intrusion detection systems are a new approach (compared to existing host-based and network-based intrusion detection systems) that is discussed in [64]. The idea is to use hypervisor capabilities to improve performance over data residing in a VM.

Security Policy Management:- In [65] the authors propose a generic security management framework allowing providers of cloud data management systems

to define and enforce complex security policies through a policy management module. The user activities are stored and monitored for each storage system, and are made available to the policy management module. Users' actions are evaluated by a trust management module based on their past activities and are grouped as "fair" or "malicious". An appropriate architecture for security management which satisfies the requirements of policy definitions (such as flexibility, expressiveness, extendibility and correctness) has been implemented. The authors evaluated the proposed system on a data management system that is built on data storage.

The policy management as a service (PMaaS) to provide users with a unified control point for managing access policies in order to control access to cloud resources independently of the physical location of cloud providers was introduced by [66]. PMaaS is designed specifically to solve the issue of having multiple access control authorization mechanisms employed by cloud service providers that restrict the flexibility of applying custom access control to a particular service. For this purpose, the PMaaS architecture includes a policy management service provider that is the entry point for cloud users to define and manage the policies. The cloud service provider imports the user-defined policies and acts a policy decision point to enforce the user policies.

IV. CRITIQUES OF EXISTING PROPOSITIONS TO CLOUD COMPUTING

The propositions solution for the cloud computing were noted to have a number of security setbacks that render them ineffective in cloud computing adoption. To start with, Authentication and Authorization, authentication which is the process that allows the user to provide proof of his identity [67]. It is often done through the login method, based on the using of a username and a password. This static mechanism leaves the system vulnerable to attacks, since hackers can use many techniques, such as sniffing and guessing, to steal user passwords [68]. On the part of Identity and Access Management, using the cloud services, users can ealiy access their personal information and make it available to various services across the Internet. [69] stated that, an identity management (IDM) mechanism can help authenticate users and services based on credentials and characteristics. A key issue concerning IDM in cloud is interoperability drawbacks that could result from using different identity tokens and identity negotiation protocols. Existing password-based authentication has an inherited limitation and poses significant risks. An IDM system should be able to protect private and sensitive information related to users and processes. However, multitenant cloud environments can affect the privacy of identity information and isn't yet well understood. Confidentiality, integrity and availability losses can make a big impact in the business of the cloud computing because the data is the core component for any business. Confidentiality is one of the prime constraints for the growth of cloud computing paradigm. Users when selecting the Cloud provider must be sure that the data that is given to the provider must be confidential. Provider must protect it from other users as well as must provide surety that even provider will also not peep into the data. Typically confidentiality is maintained by the encryption of the data that has been uploaded on the server of provider. But encryption has huge drawback in performance of the system. 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. On its part, security monitoring and incident response, many companies rely on third-party cloud

services provides and may not have access to every layer in the cloud computing stack, and therefore can't gain full visibility to monitor for potential security flaws and vulnerabilities. Lastly, on Security Policy Management, according to [70], stated that even though SaaS is based on autonomous agent, its security policy is still based on pre-defined rules, which limits the detection capabilities only to those attacks that are already known with the loud computing.

V. PROPOSED SECURITY MODEL OF CLOUD COMPUTING

The study proposed a cloud model mapped with security parameter used to enhanced the data and privacy of cloud computing. The layers in the proposed cloud security model includes; first the user creates a local agent, and establish a temporary security certificate then use this certificate for secure authentication in an effective period of time. The certificate includes the credentials such as the host name, user name, user id, start time, end time and security attributes etc. which are used access and authorization in cloud computing. Second, when the user's task use the resource on the cloud service layer, mutual authentication take place between user agent and specific application, while the application check if the user agent's certificate is expired, a local security policy is mapped. Third, according to user's requirements, cloud application will generate a list of service resource, and then pass it to the user agent. Through security API, user agent connects specific services. The cloud connection security ensures the safety of resources provided by the resource layer. The security API in this model should be achieved with SSL method, while the realization of cloud connection security uses SSL and VPN methods. The proposed security model is given in figure 4. The model consists the following security parameters:

Verification and Validation- This unit is required in cloud computing not only to authenticate users but also to ensure the accuracy of data and services on the cloud. The significance of security module is that cloud computing position is reachable by several customers and providers which want to use or provide many services and applications. Cloud service providers need to prove to the users that the services and data are valid, for example, appropriate signature algorithms. Consequently, user will be able to verify the authenticity of facts and services made available to them through digital signature. This protection part can also provide work for techniques such as One Time Password [71].

Security Policies:- Security policies are the basis of a resonance safety completion. Frequently organizations implement technical security solutions without creating foundation of policies, standards and security policies on firewall. Standards, procedures and guidelines referred to as policy in the superior sense of a worldwide information security policy [72]. Privilege Control- This security component is necessary to control cloud usage by different individuals and organizations. It protects user's privacy and ensures data integrity and secrecy by applying an anthology of rules and policies. Cloud users are granted different levels of access permissions and resource ownerships based on their account type. Only authorized users can access the authorized parts of the encrypted data through identity-based decryption algorithm. For example, in a healthcare cloud, not all practitioners have the same privileges to access patient's data, this may depend on the degree to which a practitioner is involved/specialized in treatment; patients can also allow or deny sharing their information with other healthcare practitioners or hospitals [73]. Encryption/Decryption algorithms [74] such as AES

and RC4 can be employed by this component to achieve confidentiality of information.

Data Protection- Data stored in the cloud storage resources may be very sensitive and critical, for example, clouds may host electronic healthcare records (EHR) which contain patients' private information and their health history [75]. They may also store critical banking information (e.g., clients account numbers, balances and transactions) or national security information. Cloud security model must protect data loss or injure by provide safe storage servers. These servers should also secure data retrieval and removal from the cloud. Securing data storage and processing is important since cloud users have no idea about data location. Techniques for data protection for example truncation, redaction, obfuscation, and others are able to be used in this security component. Encryption techniques can also be employed for data security. Hash functions and Message Authentication Code (MAC) can be employed in this unit to provide data integrity [76].

Security Services- The additional factors that directly affect cloud software assurance include authentication, authorization, auditing and accountability are used in cloud security services) [78]. Security-as-a- service is an industry form which a service contributor integrates security services into a commercial infrastructure on a subscription basis.

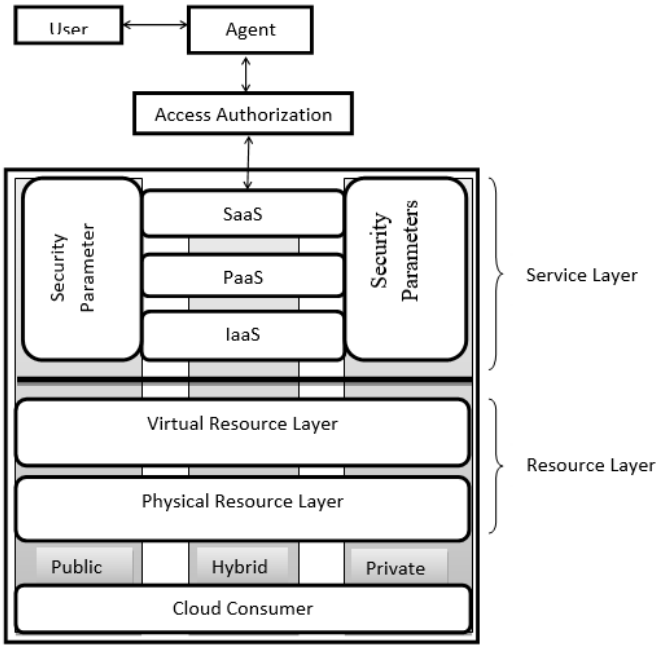

Figure 5. Proposed Security Model of Cloud Computing

Security-as a-service has applications such as anti-virus software delivered over the internet however the term can in addition pass on to security administration provided in-house by an external organization.

Threats / Attacks Detections- Clouds are vulnerable to many attacks and malicious behaviors that threaten both data and physical and virtual computing resources of the cloud. Basically, any set of actions that threaten the cloud security requirements (e.g., integrity, confidentiality and availability) are considered to be attacks. Attacks detection and prevention components are installed within the cloud security system to protect cloud resources from various anomalies. For example, denial-of-service attacks should be reduced to the minimum to guarantee the maximum availability of business, government, health and other critical information and services. This can be achieved by deploying technologies that provide high availability such as dynamic server load balancing and active/deactivate clustering [79]. Standard Distributed

Denial of Services (DDoS) mitigation techniques such as synchronous cookies and connection limiting can also be used. There are provisions for the next generation of intrusion detection systems and firewalls in order to protect the resources from intruders, viruses and malware [80].

VI. CONCLUSION

The aim of this paper is to carry out a holistic empirical study on cloud computing ecosystem security issues which hinders its adoption. It has been noted that most of the models such as delively model, service model and the enabling technologies of cloud computing that include virtualization and network are exposed to various security issues. The study further reviewed some of the security propositions of cloud cloud computing and their vulnerabilities. Based on these security setbacks, a novel security model has been proposed with some key parameters that can maintain both data integrity and confidentiality by deterring an illicit access to cloud data hence improve security.

VII. REFERENCES

[1]. P. Mell and T. Grance, (2011). The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Sep-2011.

[2]. T. Rajesh and P. Vihari, (2013). Efficient Appraisal of Cloud Computing Through Comprehensive Confrontation of Security Issues and Discrepancies Involved. International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5- May 2013

[3]. O. Kuyoro, F. Ibikunle and O. Awodele (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[4]. G. Shivani, (2017). Reviewing Security Concerns in Cloud Environment. International Journal of Computer Science and Mobile Computing, Vol.6 Issue.6, June- 2017, pg. 200-206

[5]. K. Wagh, (2014). Securing Data Transfer in Cloud Environment. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 5(Version 2), May 2014, pp.189-193

[6]. G. Bernd et al, (2011). Understanding Cloud Computing Vulnerabilities. IEEE, 1540- 7993/11, 2011, pp: 50-57

[7]. R. Balasubramanian and M. Aramudhan, (2012). Security Issues: Public vs Private vs Hybrid Cloud Computing. International Journal of Computer Applications (0975 – 8887) Volume 55– No.13, October 2012

[8]. D. Dikaiakos, et al. (2009). "Cloud computing: Distributed internet computing for IT and scientific research." Internet Computing, IEEE 13(5): 10-13.

[9]. Wayne A. Pauley,(2010) .Cloud Provider Transparency – An empirical evaluation. IEEE computer and reliability societies, IEEE, November 2010, pp: 32 – 39.

[10]. P. Wayne, (2010). Cloud Provider Transparency – An empirical evaluation the IEEE computer and reliability societies. IEEE, November 2010, pp: 32 – 39.

[11]. T. Hassan et al. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE security and privacy, www.computer.org/security, 2010, pp. 24 – 31

[12]. R. Kui et al, (2010). Security Challenges for the Public Cloud. IEEE Press, 2012, pp. 69 – 73.

[13]. T. Hsin-Yi, (2012). Threat as a Service? Virtualization's impact on Cloud Security. IEEE, IT Pro, 2012, pp: 32- 37

[14]. R. Balasubramanian and M. Aramudhan (2012). Security Issues: Public vs Private vs Hybrid Cloud Computing. International Journal of Computer

Applications (0975 – 8887) Volume 55– No.13, October 2012.

[15].W. Cong et al, (2011). Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data. IEEE transactions on parallel and distributed systems, IEEE, Digital Object Indentifier 10.1109/TPDS.2011.282, 2011, pp: 1 – 14

[16].B. Marjory,(2010) .Hide and Seek in the Cloud. IEEE, March – April 2010, pp: 57-58.

[17].P. Mell, and T. Grance, (2009). The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology Special Publication 800-145, National Institute of Standards and Technology, 2009.

[18].D. Owens, (2010). Securing elasticity in the Cloud. Commun ACM 53(6):46–51

[19].B. Tang, R. Sandhu, and Q. Li, (2013). Multi-tenancy authorization models for collaborative cloud services. in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.

[20].S. Subashini and V. Kavitha (2011). A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11

[21].Ju et al, (2010) Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387.

[22].Grobauer, T. Walloschek, and E. Stocker E (2011). Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2):50–57

[23].Cloud Security Alliance (2012). Security guidance for critical areas of Mobile Computing. Available: https://downloads.cloudsecurityalliance.org/initiatives/ mobile/Mobile_Guidance_v1.pdf

[24].M. Leandro et al,(2012). Multitenancy authorization system with federated identity for cloud-based environments using shibboleth. in Proceedings of the 11th International Conference on Networks, ICN 2012, pp. 88–93, 2012.

[25].M. Stihler et al, (2012). Integral federated identity management for cloud computing. in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, pp. 1–5, May 2012.

[26].Z. Wenjun,(2010). Integrated Security Framework for Secure Web Services. IITSI 2010, pp. 178-183

[27].B. Wang, et al (2009). Open Identity Management Framework for SaaS Ecosystem. ICEBE '09. pp. 512-517.

[28].B. Sumitra, C. Pethuru, and M. Misbahuddin, (2014). A Survey of Cloud Authentication Attacks and Solution Approaches. International Journal of Innovative Research in Computer and Communication Engineering, pp. 1-9, 2014.

[29].C. Klein, (2014). Improving cloud service re silience using brownout-aware loadbalancing. in Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on, pp. 31–40, Oct 2014.

[30].R. Popa, (2011). Enabling security in cloud storage slas with cloudproof. in Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference, USENIX ATC'11, (Berkeley, CA, USA), pp. 31–31, USENIX Association, 2011.

[31].L. Almutair and H. Zaghloul, (2013). In Proceedings of the The Third International Conference on Digital Information Processing and Communications (ICDIPC '13), pp. 676–686, UAE, 2013.

[32].J. Shropshire, (2014) "Analysis of monolithic and microkernel architectures: Towards secure hypervisor design," in Proceedings of the 47th

Hawaii International Conference on System Sciences, HICSS 2014, pp. 5008–5017, usa, January 2014.

[33]. N. Santos, K. Gummadi, and R. Rodrigues, (2009). Towards trusted cloud computing. in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[34]. R. Banyal, P. Jain, and V. Jain,(2013). Multi-factor authentication framework for cloud computing. in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.

[35]. P. Tabakki et al. (2010). SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments. Proc. 1st IEEE Int'l Workshop Emerging (2012

[36]. K. Steve et al, (2012). The Future of Authentication. IEEE, January-February 2012, pp: 22 – 27

[37]. M. Jensen, (2009). On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing, pp: 109 – 116.

[38]. Q. Sara and K. Kausar, (2012)"Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.

[39]. S. Roschke, et al., (2009). Intrusion Detection in the Cloud. IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009.

[40]. A. Elmustafa and E. Rasha, (2015). Network Denial of Service Threat Security on Cloud Computing A Survey. IJSRSET | Volume 1 | Issue 5 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099

[41]. D. Perez-Botero, J. Szefer, and R. Lee, (2013). Characterizing hypervisor vulnerabilities in cloud computing servers," in Proceedings of the 2013 International Workshop on Security in Cloud Computing, Cloud Computing '13, (New York, NY, USA), pp. 3–10, ACM, 2013.

[42]. L. Ertaul, S. Singhal and S. Gökay, (2010). Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42

[43]. Q. Sara and K. Kausar, (2012)"Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.

[44]. G. Grispos, B. Glisson, and T. Storer, (2013). Cloud Security Challenges: Investigating Policies. Standards, and Guidelines in a Fortune 500 Organization", 21st European Conference on Information Systems, 5-8, 2013

[45]. A. Jasti et al, (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41.

[46]. Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007.

[47]. K. Owens, (2009). Securing Virtual Computer Infrastructure in the Cloud. white paper, Savvis Communications Corp., 2009

[48]. A. Jasti et al.,(2010) "Security in Multi-Tenancy Cloud," Proc. IEEE Int'l Carnahan Conf. Security Technology (ICCST 10), IEEE Press, 2010, pp. 35–41.

[49].H. Takabi and J. Joshi, (2012). Policy management as a service: An approach to manage policy heterogeneity in cloud computing environment," in System Science (HICSS), 2012 45th Hawaii International Conference on, pp. 5500–5508, Jan 2012.

[50].N. Mimura et al,(2013). A framework for authentication and authorization credentialsin cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.

[51].R. Banyal, P. Jain, and V. Jain,(2013). Multi-factor authentication framework for cloud computing. in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.

[52].R. Lomotey and R. Deters,(2013). Saas authentication middleware for mobile consumers of iaas cloud. in Services (SERVICES), 2013 IEEE Ninth World Congress on, pp. 448–455, June 2013.

[53].H. Kim and S. Timm, (2014). X.509 authentication and authorization in fermi cloud. in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 732–737, Dec 2014.

[54].B. Tang, R. Sandhu, and Q. Li, (2013). Multi-tenancy authorization models for collaborative cloud services. in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.

[55].M. Leandro et al,(2012). Multitenancy authorization system with federated identity for cloud-based environments using shibboleth. in Proceedings of the 11th International Conference on Networks, ICN 2012, pp. 88–93, 2012.

[56].M. Stihler et al, (2012). Integral federated identity management for cloud computing. in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, pp. 1–5, May 2012.

[57].N. Santos, K. Gummadi, and R. Rodrigues, (2009). Towards trusted cloud computing. in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[58].T. Garfinkel, (2003). A virtual machine-based platform for trusted computing. in Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, SOSP '03, (New York, NY, USA), pp. 193–206, ACM, 2003.

[59].R. Popa, (2011). Enabling security in cloud storage slas with cloudproof. in Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference, USENIX ATC'11, (Berkeley, CA, USA), pp. 31–31, USENIX Association, 2011.

[60].S. Zhu and G. Gong, (2014). Fuzzy authorization for cloud storage," Cloud Computing, IEEE Transactions on, vol. 2, pp. 422–435, Oct 2014.

[61].C. Klein, (2014). Improving cloud service re silience using brownout-aware loadbalancing. in Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on, pp. 31–40, Oct 2014.

[62].E. Lakew, (2014). A synchronization mechanism for cloud accounting systems," in Cloud and Autonomic Computing (ICCAC), 2014 International Conference on, pp. 111–120, Sept 2014.

[63].M. Anand, (2012) .Cloud monitor: Monitoring applications in cloud. in Cloud Computing in Emerging

[64].Markets (CCEM), 2012 IEEE International Conference on, pp. 1–4, Oct 2012.

[65].A. Brinkmann, (2013). Scalable monitoring system for clouds. in Proceedings of the 2013 IEEE/ACM 6th International Conference on

Utility and Cloud Computing, UCC '13, (Washington, DC, USA), pp. 351–356, IEEE Computer Society, 2013.

[66].C. Basescu, (2011). Managing data access on clouds: A generic framework for enforcing security policies. in Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, pp. 459–466, March 2011.

[67].H. Takabi and J. Joshi, (2012). Policy management as a service: An approach to manage policy heterogeneity in cloud computing environment," in System Science (HICSS), 2012 45th Hawaii International Conference on, pp. 5500–5508, Jan 2012.

[68].H. Chang and E. Choi, (2011). User authentication in cloud computing. in International Conference on Ubiquitous Computing and Multimedia Applications, pp. 338–342, 2011.

[69].B. Sumitra, C. Pethuru, and M. Misbahuddin, (2014). A Survey of Cloud Authentication Attacks and Solution Approaches. International Journal of Innovative Research in Computer and Communication Engineering, pp. 1-9, 2014.

[70].S. Jaydip (2013). Security and Security andPrivacy Privacy Privacy Issues in Cloud Computing Computing. Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[71].K. Issa , K. Abdallah and A. Muhammad (2014).Cloud Computing Security: A Survey. Cloud Computing Security: A Survey.

[72].E. Ahmed et.al. (2012). A Framework for Secure Cloud Computing. IJCSI International Journal of Computer Science, Vol. 9, issue 4, No 3, ISSN (Online): 1694-0814, July 2012.

[73].R. Krutz et.al. (2013) .CLOUD SECURITY Comprehensive Guide to Secure Cloud Computing. Chapter 2: Cloud Computing Architecture, WILEY-INDIA, ISBN : 978-81-265-2809-7.

[74].R. Zhang and L. Liu, (2010) .Security Models and Requirements for Healthcare Application Clouds. IEEE 3rd International Conference on Cloud Computing.

[75].Leonard D.C. et.al.(2009) "Realization of Universal Patient Identifier for Electronic Records through Biometric Technology", IEEE Trans on Information Technology in Biomedicine, Vol. 13, No. 14.

[76].E. Ahmed et.al.(2012). A Framework for Secure Cloud Computing. IJCSI International Journal of Computer Science, Vol. 9, issue 4, No 3, ISSN (Online): 1694-0814, July 2012.

[77].A. Tripathi and A.Mishra (2011). Cloud Computing Research Challenges. IEEE 5th International conference on Biomedical Engineering and Informatics, pp- 1397-1401.

[78].R. Krutz et.al.(2013). CLOUD SECURITY Comprehensive Guide to Secure Cloud Computing. Chapter 2 : Cloud Computing Architecture, WILEY-INDIA, ISBN : 978-81-265-2809-7.

[79].A. Tripathi and A. Mishra (2011). Cloud computing security considerations. IEEE International conference on signal processing, communication and computing (ICSPCC).

[80].A. Mohiuddin et.al.(2012). An Advanced Survey on Cloud Computing and State-of-the-art Research Issues. IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, vol. 9, issue 1, No 1.