IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Survey on Cloud Security Issues and Challenges

S.Indhumathi[1],T.Manigandan[2], S.T.Saravanan[3]

Assistant Professor Department of CSE, Bharathiyar Institute of Engineering for Women, Salem, India[1]

Assistant Professor, Department of CSE, SRS College of Engineering and Technology, Salem, India[2]

Assistant Professor Department of CSE, Bharathiyar Institute of Engineering for Women, Salem, India[3]

Abstract: A rapidly expanding service, cloud computing security offers many of the same features as traditional IT security. This includes preventing data loss, leakage, and theft of important information. Scalable operations without sacrificing security are one advantage of cloud services. Though you now have new methods for offering security solutions that target new areas of concern, it is comparable to how you presently handle security. Cloud security does not alter the security management methodology from preventive to investigative and remedial measures. However, it does enable you to carry out these tasks with greater agility. This study examines the general cloud architecture and the difficulties in creating the cloud Secure.

Keywords: Traditional IT security, cloud services, Cloud security, cloud architecture.

I. INTRODUCTION

Premeditated or inadvertent data exposures have plagued cloud computing history. This reveals the issues related to privacy and cloud data storage deployment privacy. The first danger kind ever is inadvertent data leakage, which arises from mistakes in the providers' cloud computing software's architecture.

For example, a defect in Google Docs allowed non-authenticated individuals to read the documents. Premeditated or inadvertent data exposures have plagued the history of cloud computing. This reveals the privacy and security dangers associated with the introduction of cloud data storage. The first danger kind ever is inadvertent data leakage, which arises from mistakes in the providers' cloud computing software's architecture. For example, a defect in Google Docs allowed non-authenticated individuals to read the documents, while weaknesses in Facebook and Flickr also allowed users' private photos to be released [2].

Internet computing is all that cloud computing is. The term "cloud computing" refers to the use of the internet to offer technology-enabled services to individuals and businesses, as the internet is typically perceived as a collection of clouds. These days, cloud computing is a new tool that many businesses are attempting to implement to enhance their workflow. In order to manage applications, it entails sharing computing resources. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) are three examples of the services that cloud computing offers at different abstraction levels. It also offers lower capital expenditure, operational risks, complexity and maintenance, and enhanced scalability. Applications geared toward the customer, like financial portfolios that provide tailored information or powerful, immersive video games, leverage it. Due to the pay-per-use nature of the service, it has gained a lot of popularity quickly.

We must fully comprehend the compound security concerns before we can comprehend cloud security issues. In particular, we must: (i) look into different aspects of cloud security, such as vulnerabilities, risks, attack models, and threats; (ii) determine the security requirements, such as privacy, integrity, availability, and transparency; (iii) identify the parties involved, such as clients, service providers, outsiders, and insiders, and their respective roles in the attack-defence cycle; and (iv) comprehend how security affects different cloud deployment models, such as public, community, private, and hybrid.

This paper's primary contribution is a comprehensive analysis of cloud security issues that covers nearly all cloud stakeholders (providers, consumers, third-party contractors, etc.), network layers (application, transportation, IP, etc.), and cloud components (data centres, computing infrastructure, interacting and networking, etc.).

Our survey covers a wide range of topics related to cloud security and privacy, such as: (i) threats, vulnerabilities, and attacks related to cloud computing; (ii) attack classifications; (iii) relationships and dependencies between attacks; (iv) known attacks; (v) a comparative analysis of some popular countermeasures; and (vi) insights from current security solutions to identify and address unattended security challenges. A typical cloud-based scenario with the cloud service provider and cloud users in a cloud computing architecture is shown in Figure 1.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

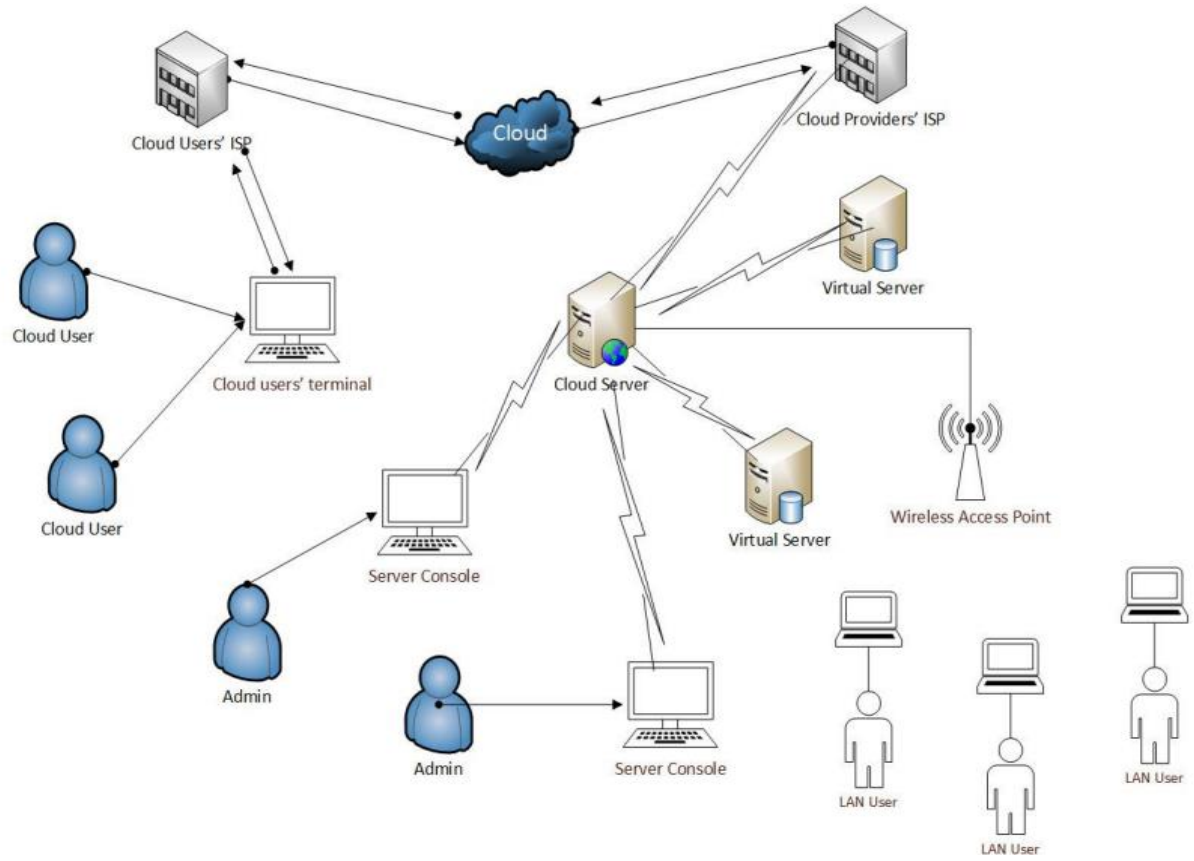

Figure 1: A Typical Cloud Architecture

Figure 1 presents a simplified cloud architecture illustration that omits some of the more intricate aspects of cloud computing, such as geographic dispersion of the cloud provider's network, server replication, and redundancy. The illustration's main goal is to establish the arrangement that turns the concept of cloud computing into a tangible one. When the network architecture is seen in the context of the discussion of the cloud computing idea, it becomes evident how cloud users are identified... A noteworthy feature of the architecture is that, although the cloud users are named and identified appropriately based on their remote location and method of remote access to the cloud servers, the admin users who manage the cloud servers are not considered cloud users in any way concerning the network of the cloud service provider in the given scenario. Whether or not the LAN users in Figure 1 are cloud users is debatable. Because "cloud computing" is a concept rather than a technical term, there may be room for disagreement. The LAN users in Figure 1 might not be regarded as cloud users in this context if the notion of cloud computing is understood to include the distantly situated servers that are accessed through public infrastructure (or the cloud). The LAN users in this scenario are essentially cloud users when they use the servers' cloud services; from this perspective, the LAN users are essentially using resources that are "borrowed" from the servers on an as-needed basis. Distributed and grid computing are the mother technologies that define the infrastructure approach to achieve cloud computing.

On the other hand, due to bugs, Facebook and flicker have also revealed user private photos [4].

All that cloud computing is, is internet computing. Since the internet is typically thought of as a collection of clouds, cloud computing can be defined as using the internet to give people and businesses access to technology-enabled services. A new tool of this period that many businesses are hoping to implement to enhance their workflow is cloud computing. It suggests pooling computer power to run programmes. Cloud computing provides services at various abstraction levels, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and more, with less capital outlay, operational hazards, complexity, and upkeep. AndIaaS, or infrastructure as a service. It powers immersive computer games and financial portfolios that provide tailored information, among other consumer-focused applications. Because it is a pay-per-view service, it has gained a lot of popularity quickly [6].

We must fully comprehend the compound security concerns before we can comprehend cloud security issues. In particular, we must: (i) look into different aspects of cloud security, such as vulnerabilities, risks, attack models, and threats; (ii) determine the security requirements, such as privacy, integrity, availability, and transparency; (iii) identify the parties involved, such as clients, service providers, outsiders, and insiders, and their respective roles

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

in the attack-defence cycle; and (iv) comprehend how security affects different cloud deployment models, such as public, community, private, and hybrid. This paper's primary contribution is a comprehensive analysis of cloud security issues that covers nearly all cloud stakeholders (providers, consumers, third-party contractors, etc.), network layers (application, transportation, IP, etc.), and cloud components (data centres, computing infrastructure, interacting and networking, etc.). Our survey covers a wide range of topics related to cloud security and privacy, such as: (i) threats, vulnerabilities, and attacks related to cloud computing; (ii) attack classifications; (iii) relationships and dependencies between attacks; (iv) known attacks; (v) a comparative analysis of some popular countermeasures; and (vi) insights from current security solutions to identify and address unattended security challenges. In a cloud computing architecture, the cloud service provider and the cloud users are depicted in Figure 1 as a typical cloud-based scenario [8].

Figure 1 presents a simplified cloud architecture illustration that omits some of the more intricate aspects of cloud computing, such as geographic dispersion of the cloud provider's network, server replication, and redundancy. The illustration's main goal is to establish the arrangement that turns the concept of cloud computing into a tangible one. When viewed in conjunction with the explanation of the cloud computing idea, the network architecture and cloud user identity are self-explanatory [11].The architecture is noteworthy in that the admin users who are managing the cloud servers are not considered cloud users in any way with regard to the cloud service provider's network in the scenario, even though the cloud users are named and clearly identified as such because of their remote locations and means of remote access to the cloud servers. Whether or not the LAN users in Figure 1 are cloud users is debatable. Because "cloud computing" is a concept rather than a technical term, there may be room for disagreement. .. The LAN users in Figure 1 might not be regarded as cloud users in this context if the notion of cloud computing is understood to include the distantly situated servers that are accessed through public infrastructure (or the cloud). The LAN users in this scenario are essentially cloud users when they use the servers' cloud services; from this perspective, the LAN users are essentially using resources that are "borrowed" from the servers on an as-needed basis. Distributed and grid computing are the mother technologies that define the infrastructure approach to achieve cloud computing.

II. THE GENERIC ARCHITECTURE

The client module and the server module make up the two components that make up the generic architecture. The model's overall description can be seen in the following figure.

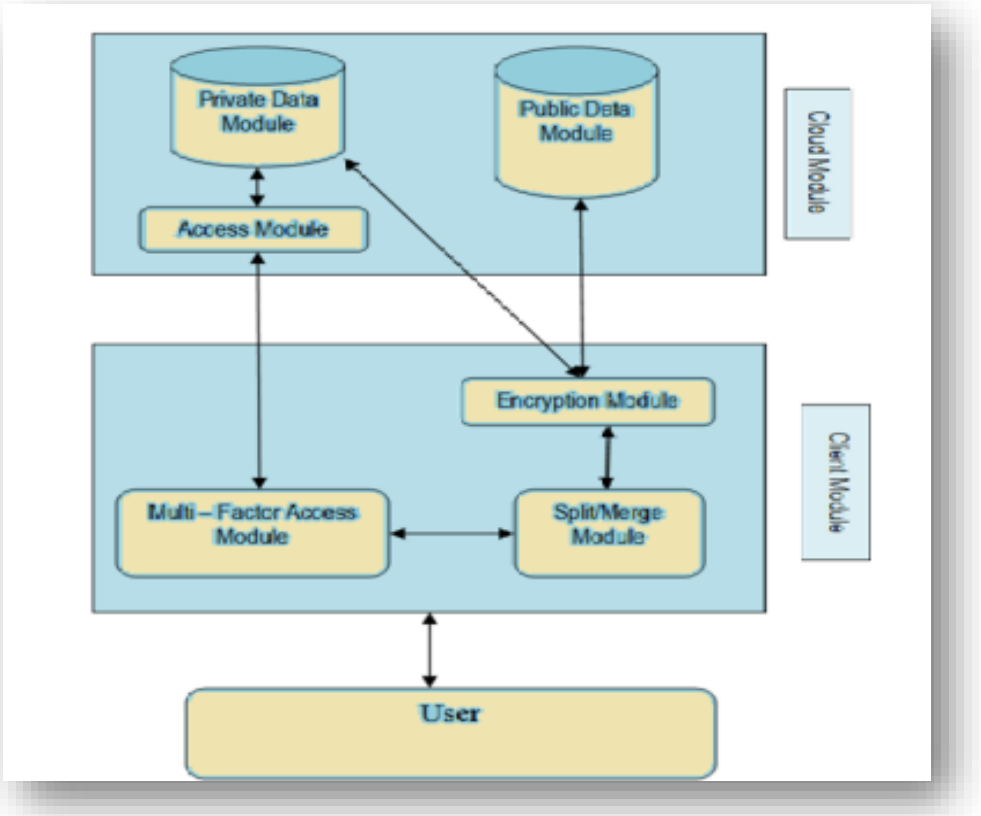

Fig 2: Generic Architecture

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

2.1 The Module for Clients

There are three key parts to the client module. The components for split and merge, access control, and encryption and decryption. Each component's operation is described in detail.

2.1.1. Client Access Control Component:

The access control component manages the cloud user's authorization and authentication. A user name and password constitutes the most basic authentication technique available. However, this authentication mechanism is insufficient for cloud computing. The user will enter their username and password to log in, and the cloud access control component will randomly generate the two session passwords. One is forwarded to the user's official email address, and the other is forwarded to their mobile phone. With the use of these two session passwords, the user may be verified. After authentication is finished, the access control module will disappear into the background, and components that split, combine, encrypt, and decrypt data will be used for the remaining data access and storage.

2.1.2. The Split and Merge Component:

The user will be able to use cloud data storage services following authentication. The data will initially be separated using the split algorithm when the client requests to send data. The original data form can be viewed by using the merging technique once the data has been received. The data is divided into even and odd pieces by the split algorithm, which is followed by the reverse process of the merging algorithm.

2.1.3. Encrypt/Decrypt Component:

The data is sent to the encrypt/decrypt component following its splitting by the split and merge component. After using AES encryption techniques, the encrypt/decrypt component sends the encrypted data to a cloud storage server. The data is kept in the server's public component, while the key is kept in the private data component. The same method is applied when the data is sought back from the storage. After decrypting the data, the key is extracted from the private data component and the data from the public data component is returned to the split and merge component, where the merging algorithm is applied to produce the original data.

2.2. The Module for the Server

Our architecture's cloud server module is also made up of three parts. These parts consist of the public data component, the private data component, and the authentication component. The following describes how these parts function.

2.2.1 Authentication Component:

The server module's private data component and the authentication component collaborate closely. Authentication module is responsible for randomly generating two session passwords and sending one to the user's official email account and the other to their cell phone number when the server gets a request for authorization of data access. After verifying the user's session passwords, the user is authorised.

2.2.2. Private Data Component:

This component handles more than just storing user credentials (Login Information). However, it is also in charge of keeping the secret keys that are required to decrypt the data stored in the cloud storage's public area stored. The private data area of the cloud storage can only be accessed by the data owner, who can then update, remove, or append data. The secret data sector is not accessible to the user for data operations.

2.2.3. Public Data Component:

All authorised users of the particular data will have access to the data that is stored in the public component. Every piece of information kept in the public data part will be available in encrypted form. In addition to creating the data in this component, the owner is also in charge of the various data operations.

III. PROBLEMS WITH SECURITY IN CLOUD COMPUTING

Cloud Implementation Model Security In essence, a cloud's deployment is either controlled internally (Private Cloud) or remotely (Public Cloud). However, it is implemented as an integrated private-public cloud (Hybrid Cloud) for a variety of reasons. A fourth category of cloud implementation methods is called a "Community Cloud," in which a particular community can utilize technology that is distributed across multiple organizations. The aforementioned figure displays the various cloud implementation models. An organization using a private cloud configuration can choose to be physically on-site or off-site in charge of its infrastructure, or it can give that authority to a third party. There is no need for additional trust mechanisms because the security of the internal cloud architecture can be managed. However, there are a number of concerns with having a third-party service provider manage the private cloud. A private cloud solution is chosen by users in order to boost security. As a result, there is less segregation between the infrastructure and the services. Taking care of the offered service's security, for example, when working with the current firewalls and security services [13]. Moreover, one way to separate the private cloud hosted by a third party is to use a secure virtual private network. Even with a private cloud's advantages, there are a few problems that need to be fixed, such as uneven resource usage. For instance, a slow infrastructure wastes resources.

3.1 Cloud security challenges

It appears that enterprises must overcome a number of obstacles before deciding to adopt cloud computing.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

The current state of cloud services offers numerous ways to solve issues. Among others, security issues, viability, and interoperability are a few to mention. Some writers have offered plausible solutions to the different problems, but few scholars have emphasized the need for more advancements. When thinking about using an external outsource to store their data and procedures, security is a major concern. The worries go beyond the possibility of data loss and corruption to include issues with service availability, trust, and unforeseen problems.

A few examples of the availability issue include Google service outages that occurred in 2008, ranging from 1.5 to 8 hours. A small number of authors have outlined ten obstacles to cloud computing's growth and some avenues for resolution. One of the challenges is data privacy, for which data encryption is recommended as a potential solution. Few authors have emphasized the necessity of taking significant action to strengthen cloud security. The guarantee provided by the Service Level Agreement (SLA), which is a contract between the service provider and the users, is one of the suggestions. However, among the several alternatives put forth is a "multi-tenancy" support that enables users to adjust to the specific context they want thanks to customized security settings.

Justifying the pricing model in terms of cloud services is difficult. Customers of cloud services must consider a variety of trade-offs with relation to the price of integration, connectivity, processing power, and security measures. Data transfer and connectivity costs will be used in place of the infrastructure costs. Limiting the expense of communication is unavoidable because of the heavy reliance on frequent, massive data transfers. Considering the unique scenario of hybrid clouds, where ongoing data movement between the public cloud, internal IT infrastructure, and the private cloud is necessary. The managerial choices of choosing an appropriate costing model based on the available possibilities were not extensively covered by writers.

Additionally, they mentioned that, in contrast to the expensive expense of in-house infrastructure, on-demand services provide companies with affordable usage-based rates. Cloud services will either connect with or replace internal infrastructure, therefore the charge-back strategy needs to be carefully considered. When compared to the creation of legacy infrastructure, cost analysis becomes more intricate. Three areas—storage, access, and processing costs—were suggested by one author as ways to bill clients via the cloud. This broadens the scope of the analysis when taking into account a public cloud service. However, creating a safe architecture will require additional optimization in order to reduce the cost of using a public cloud. To improve return on investment, one option to consider is a hybrid cloud.

SLA is a crucial consideration for public cloud services, as shown in. Obtaining a guarantee is crucial prior to engaging in significant business activities involving external resources. It is anticipated that the supplier to guarantee the performance, dependability, accessibility, and availability of the service. The interpretation of the terms and the standards for evaluating them are two potential issues with the agreements. While this can lead to confusion, it also means that the terms might not include what the customers need or expect. Additionally, the terminologies for various cloud providers, such as Iaas, Paas, and Saas, differ and add to the complexity of the SLA. In order to do this, the SLAs must be both mutually understood and flexible enough to adjust to the unique needs of the customer. Automated SLAs attempt to address these issues, however as noted, in practice it is challenging. Selecting what to move to the cloud can be difficult, and users may be unsure about their choices. Migration decisions are constrained by trust and security concerns, even in the face of declining capital and operating expenses. According to the findings of a study that one author gave, security is the main issue. According to IDC's analysis, there will be a significant rise in spending to construct public clouds by 2014, with an estimated 55.5 billion US dollars. The development of apps will take up more than half of the budget, with infrastructure, servers, and storage coming in second. However, migration is anticipated to be more likely in the direction of SaaS, with IaaS and PaaS following suit. It might be difficult to get internal systems and data to work with cloud services. Data lock-in is a concern brought up by the absence of a common interface. Moreover, it can be difficult or even impossible to grow the cloud services, even by using many clouds. Using a hybrid cloud strategy brings up numerous issues with data and operation compatibility [14]. Without shared standards, integrating public and private clouds hinders a seamless and rapid spread of the cloud. A few writers emphasized the necessity of standardizing the security problem, maybe through the adoption of a carefully thought-out security standard. Consequently, standardizing APIs is suggested as a solution in various papers, making it simpler to migrate between clouds or services.

IV. SUMMARY

Utilizing the current technology has seen a fundamental shift in cloud computing. As a society, the tendency to use cloud services appears to be growing in importance. The cycle of presenting additional technological advances is getting smaller, especially in this day and age. Organizations should think about utilizing cloud services as an essential component of their operations for a variety of reasons, one of which is the reduction of capital costs. Nonetheless, a number of obstacles are preventing widespread placement and recognition from being implemented. The inability of the current cloud service implementations to provide a high security level is their main flaw.

DOI 10.17148/IJARCCE.2017.63243

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Furthermore, security assertion requires coverage of the transmission channels that impact the inclusion of a third party. Many concerns need to be improved in order to guarantee high levels of security, privacy, authenticity, incorporation, speed, scalability, and trustworthiness in order to properly utilize cloud services. An automatic SLA, a third-party trusted source, or a fresh development can make for an interesting research topic to address cloud computing security concerns.

REFERENCES

[1]. Sangita Rani Satapathy, AnupamTripathy, Piyush Mehta, and SarikaGupta.An encrypted and searchable cloud computing data storage system. Third IEEE International Conference on Advance Computing (IACC), 2013, IEEE.
[2]. ElhamShamsinezhad, Ahmad KhademZadeh, ElrezaHedayati, and Hamid Banirostam A Trust-Based Method for Boosting Cloud Computing Infrastructure Security. The fifteenth international conference on computer modeling and simulation, UKSim 2013, was held
[3]. ZhengXuefeng and Sultan Ullah. A Reliable Storage Architecture for Cloud Computing is called TCLOUD. Vol. 63, 2014, International Journal of Advanced Science and Technology.
[4]. Ahmed Monjur1 and Ashraf Hossain, Muhammad. Cloud computing and cloud security concerns. January 2014 issue of International Journal of Network Security & Its Applications (IJNSA), Vol. 6, No. 1.
[5]. Physician P.K. Rai, R.K. Bunkar, and Vivekananda Mishra. Concerns about Data Security and Privacy in Cloud Computing. IOSR Journal of Computer Engineering (IOSR-JCE) Volume 16, Issue 1, Ver. IX (Feb. 2014), e-ISSN: 2278-0661, p-ISSN: 2278-8727.
[6]. YogitaPawar and Mr.PrashantRewagad. Digital Signature Utilization with Diffie Hellman Using the AES encryption algorithm and key exchange, cloud computing can improve data security. International Conference on Network Technologies and Communication Systems, 2013.
[7]. Muahad M. Abu-Faraj, HossamFaris, RubaObiedat, Bader Alfawwaz, Nazeeh A. Ghatasheh, and Osama Harfoushi. A conceptual analysis and review of cloud computing's data security issues and challenges. Networks and Communications, 2014, 6, 15–21 Published February 2014 on the internet.
[8]. Dr. H S Guruprasad and S C Rachana New Security Problems and Difficulties in Cloud Computing. Volume 3, Issue 2, March 2014, International Journal of Engineering Science and Innovative Technology (IJESIT).
[9]. Muhammad Azeem, AbdallahKhreishah, and Issa M. Khalil. A survey on cloud computing security.Computers ISSN 2073-431X Computers
[10]. Sara Dadizadeh and Amit Goyal. A Cloud Computing Survey. British Columbia University, located in Vancouver.
[11]. Eduardo Fernández-Medina, Eduardo B. Fernandez, David G. Rosado, and Keiko Hashizume. an examination of cloud computing security concerns. Hashizume& Co. 2013, 4:5 Journal of Internet Services and Applications.