(IJIASE) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

AN EXPLORATION OF THE KEY INFLUENCER TO SECURITY FEATURES IN CLOUD COMPUTING FRAMEWORK AND PLATFORMS

Saumya Shikhar Raj

ABSTRACT

Objective: This paper focuses around the approaches to start specialist co-ops to make a more secure cloud platform by just verifying distributed computing servers, contributing a security scanner before sparing onto a cloud lastly before getting to a cloud provider, the utilization of a secret word or key to enter your cloud account. Strategies: This paper is broad research in the cloud security through secret phrase may be progressed, for example, biometric scanners, unique mark scanners previously utilized on most cell phones, and is seen as a sheltered method to store information on a gadget like a hard-drive. The significant unpredictability of distributed computing is security protection. Security compliances resemble insurance of information and check the utilization and pertinence of distributed computing suppliers. Discoveries: The principle topic of distributed computing has different fearless for the clients, and this office supplier with respect to security. To counter these issues, for example, the absence of a system, this disturbs a server connecting onto a distributed computing server on account of the absence of system inclusion and so forth. This can make a cloud lose the majority of its data and tragically its put away information as a cloud server may portray a framework slamming, (which can make all put away information erase, if the cloud client has not spared its information onto the cloud server) the most ideal way is if the specialist organizations of a cloud and furthermore its clients work with one another to accomplish extreme security. The best thing for a client is to report issues in regards to the cloud to their specialist co-ops (cloud and furthermore their internet services). The answer for system accessibility is basically the creation and reasonability of web office to cloud clients. Enhancements: Web clients and information office suppliers require to inspect the best approach to control issues and apply different procedures to avoid loss of sign, for example, improve their inclusion in regions difficult to reach and give progressively succinct system signal inclusion in urban zones. Truth be told, a sign enhancer has been difficult to arrive at territories, for example, rustic zones. This requires a propelled calculation from software engineers.

1. INTRODUCTION

Cloud computing is merely to put the stored informationonto a server via the use of the Internet. Nowadays, this hasbecome the norm; many people around the world, eitheryoung or old, use this to their advantage. Let's not forgetabout the power of massive industries that use clouds tostore data and sensitive information. This can be used tobasically do about anything on any device throughout theworld as long as you have a user-name and password. The basic idea is that cloud computing falls undera sort of web-based computing, in which we can shareresources, data, and information. A cloud computing providerhas various capabilities to store and process data. Cloud service providers are a demand by the pay for accessingthe cloud services. Consumers, such as enterprises, areattracted by the opportunity for reducing or eliminatingcosts associated with the "in-house"

provision of these services. Typically, these are provided through Service LevelAgreements (SLAs) brokered between the providers andconsumers. Providers like Amazon, Google, Sales force, IBM, Microsoft, and Sun Microsystems have started todevelop new data centers for hosting cloud computingapplications in various locations around the world to provide redundancy and make certain consistency. Asthe demands of the user for cloud services are varied, serviceproviders have to ensure that the flexibility in theservice delivery while keeping the users isolated from theessential infrastructure1. Cloud providers have reused theresources after relinquishing by the particular user resultingin high resource utilization2. The user-friendly environment isanother advantage of cloud computing because it does notrequire the customers to possess astonishing knowledgepertaining to cloud technologies3. Cloud computinghas behavior to earlier routes of the Internet with theidea from the American military to store its digital dataand sensitive information online, which back then was amajor development because of the cold war and againstRussia. That could be seen as a step to a safer way ofsecuring data, however back then, only a small amount ofdata was used compared to the massive Terabytes we canharness nowadays. This lead to the massive developmentof cloud computing from the 1960s to 2016. The conceptand algorithm are the same except that it's in a moreadvanced state then back then. If something is stored electronically, you must knowthat it’s easy to hack with the correct algorithm. Anyonecan be a hacker nowadays with the advancement of technology; things are becoming easy to use, accessible, andlargely most internet usage is not tracked as there is anoverload of users on a server because of all the so-called 'smart-devices.' This is making things a bit difficult forcloud service providers and especially network serviceproviders as they are dealing with new threats each andevery day. Threats become more prevalent in everydaylife, threats to any technological device that uses wirelesstechnology; this can include printers, a POS card system, mobile phones, or basically anything that is based on asystem that converts and transfers data and information. This is extremely unreliable to an invasion of any kind, virusattacks, phishing, viruses of high intent against data, andinformation.

Figure 1. Cloud computing service system

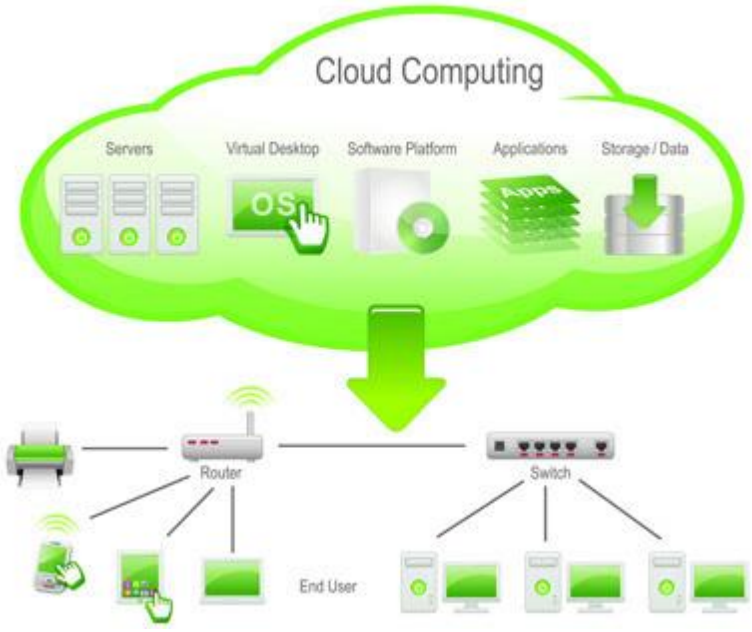

Figure 2. The layout of cloud computing operation.

(IJIASE) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

As shown in Figure 1, cloud computing devices thatcan be used to access and store data via mobile and networkservice providers. The most relevant definition isthe access to information through network and cloud serviceproviders via the web. Figure 2 explains the layout of how cloud computingservices to fulfill the customers'requirements. This canhave major and successful operations for a user, a cloudprovider, and a network service provider. Cloud computing is the fastest-growing software onthe market at the moment, with vulnerabilities, beingin its early stages of development, has caused some seriousmalfunctions of for some cloud providers, these canrange from lack of network to an actual attack againstthe user (cloud provider). But for now, the definition ofcloud computing begins with the storage of information fromhardware to software built into a server by a cloud serviceprovider4,5. The combination of Cloud Computingand IOT brings future innovations in the World WideWeb. The new thoughts coming from this integration iscalled Cloud IoT. It is new creativity in the Research andDevelopment of Cloud6.Figure 1. Cloud computing service system. Figure 2. The layout of cloud computing operation. Nowadays, cloud computing is accessed easily viamobile devices. These mobile devices have to be constantlyconnected to a network, which in turn provides you the service of storing and receiving stored data andinformation. Security plays the utmost importance intoday's day and age; we as humans need security to knowthat we are safe from harmful elements and know that wealways protected. Security is defined as "the state of beingfree from danger or threat". Transport Layer Security7has been introduced, "Secure Sockets Layer (SSL)," by 1996. Cloud computing and its securities play a majorrole in almost every form of technological existence. We, as humans, are very easily persuaded by things, which canactually harm yourself, your family, and or another person. The best defence is to create that sense of safety andalways be alert.

2. CLOUD SERVICES

There are three major cloud services, such as SaaS, PaaS, and IaaS. These are just a few reasons why it's importantalways to be aware and on the lookout. Figure 3 illustratesthe various Cloud Services provided to its users and howit operates. Figure 3. An outlook of cloud services.

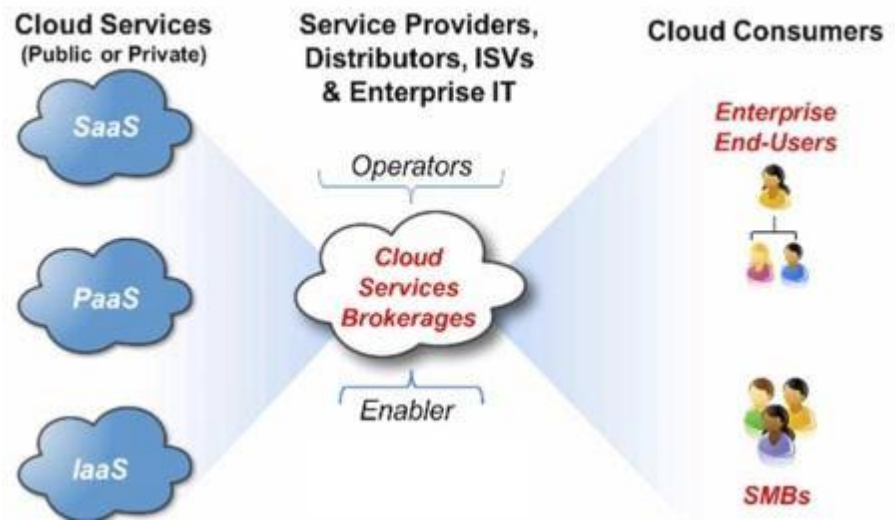

Figure 3. An outlook of cloud services.

Software as a service or SaaS:

Programming works on PC frameworks had and dealt with by the SaaS supplier, contrasted with setting up and took care of client PC frameworks. The application projects are used over the open Internet and by and large, offered on a month to month or every year membership framework. It enables the client to utilize programming as it were.

- Web access to professional software
- Program is handled from a central location
- Program provided in a "one too many" model
- Customers not required dealing with software improvements and patches
- Program Development Connections (APIs) allow for incorporation between different items of software

Platform as a service or PaaS:

All applications and components expected to make and execution cloud-based applications are given by the PaaS organization through gathering the Internet, VPN, or devoted program association. Customers pay by utilization of the program and control how applications can be utilized all through their lifecycle.

Infrastructure as a service or IaaS:

Registering, stockpiling, online networking, and different parts (security, devices) are given by the IaaS organization by means of the open Internet, VPN, or dedicated framework relationship. Clients have the freedom to possess and deal with the working framework, projects, and data running on the offices and pay by usage.

2.1 Several Areas of Concern Regarding

Security Vulnerabilities of CloudComputingThere are multiplying ways an issue such as security can bemajor regarding cloud computing, the simple idea beingthe lack of network coverage, physical error, transparency, issues regarding the providers (network and service), etc. As shown in Figure 4 explains where and what cloudcomputing is used for various computing agencies. Cloud computing is becoming more advanced, butdisturbances such as viruses, lack of network coverage, and unreliability by network service providers are causingmajor troubles for a cloud service provider and its users. Things such as:

• Lack of network coverage is a major issue regardingcloud computing as clouds require an activeinternet connection. If not, this can stop the uploadingimportant information and can, in

otherwords, lock a cloud if the provider has sensed an issue. This will cause major disruptions and securityfor a user will be open to attacks as errorswon't be or go unnoticed.

• The physical error could refer to the loss of physicalcontrol of the computer user and his cloud storage. Once the loss of data occurs, a range of problemsarises, such as privacy issues, risks, legal problemssuch as if a hacker gets hold of private info, thiscan ultimately affect a user. This will have majorconsequences on almost every concept of cloudcomputing.

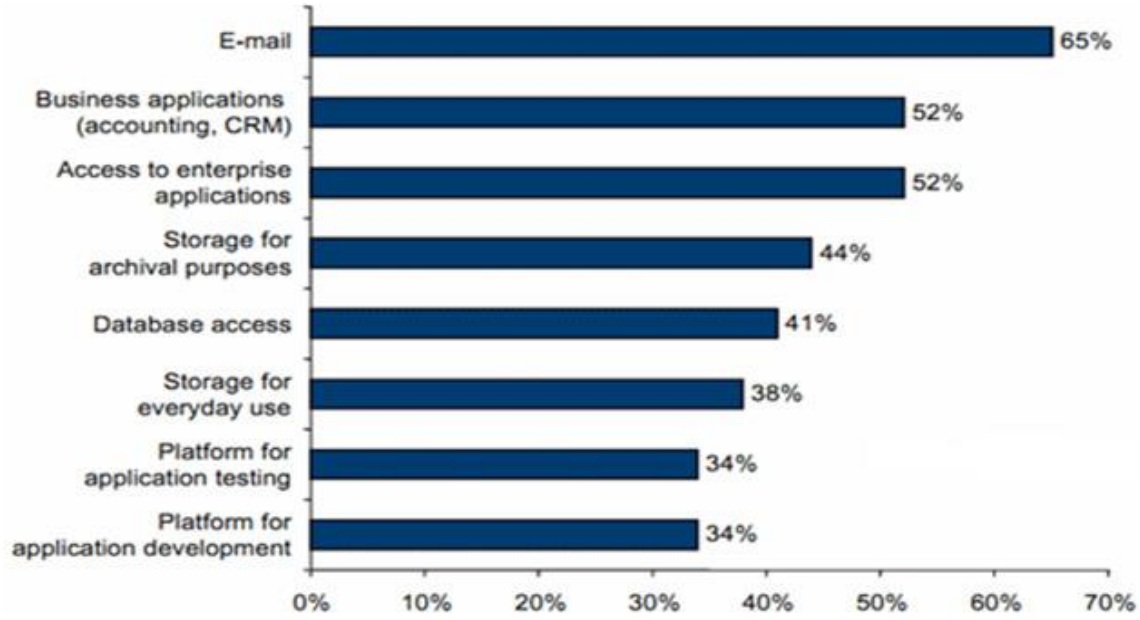

Figure 4. Uses of cloud computing.

According to Vic Winkler explained that the mainhope of cloud computing is network connectivity andbandwidth. Based on the demand, we utilize cloudstorage data. The lack of network coverage causes variousproblems in a cloud, for the user and for a serviceprovider10,11. Things can go out of proportion:

• Cloud Provider Viability: The new cloud providersdo not have technical knowledge aboutthe cloud and facing the complexity of their viability, commitment, and authenticity in the ever-growing field of technological development. Asexplained earlier, clouds are still developing, sothere might be an error or a problem there, whichis why some service providers provide a 24/7 servicecenter for users to contact in times of need. For example, Google has a 24/7 customer servicecenter, and Yahoo has standby on-demand customerservice operators.

• Transparency: Cloud providers doesn’t explicitlymention their internal protocols and technologicaladvancements, thus indirectly implementinga trust from its users as they must trust theprovider’s security claims, that it is safe and reliable. This is a major concern going un-noticednowadays as people (users) are blindly followingadvertisement.

• Loss of Physical Control: This can range fromalmost breach in protocol from users to serviceproviders not providing the needs of the user, unableto find the required data, and its applications12.It deals with the following parameters like:

• Data Privacy: In a public cloud, data does not stayon the same system, which arises the multiple legalconcerns. These legal concerns can have majorimplications against users and service providersas a whole.

• Data Control: A service provider's IT division hasless control scope within the IAAS layer implementationand still lower in the PAAS layer. Usersmust have efficient that the provider assures theoptimal control structures and solutions to allproblems arising while keeping in control whatdata is being used.

• New Risks and Vulnerabilities: The main complexityis the function of a network and cloudcomputing service provider's implementationto its users. Thus leads problems on all software, hardware, and networking equipment, whichare focusing on the detection of vulnerabilities likesecurity risks imposed on cloud computing fromvarious elements. But by simply applying layeredsecurity software's, improving the algorithm ofcloud computing elements and its operations, we can safeguard from common attacks fromincreasing security issues.

• Legal and Regulatory Compliance: Usage ofpublic cloud data subject to regulatory compliancefrom governments or organizations that arerestricting you from using some advances andtechniques while saving onto a server. Cloudproviders are to address the needs of regulatedmarkets in developed nations, while in undevelopednations, it is still in the process of restrictiondue to the lack of required skills and infrastructure. The optimal practices, development, andbetter understanding of cloud computing providea better, greater scope for development, and this concern should be able to fade away. Asshown in Figure 5, explaining the cloud computingconcerns in security risks and privacy. Figure 5. Security risks and privacy.

Figure 5. Security risks and privacy.

3. METHODOLOGY

There are ways to initiate service providers to create saferclouds by simply securing cloud computing servers. Thiscan be done in many ways and is currently the safest wayto make sure your data and information are safe becausethese use an extremely advanced algorithm, which is biometricallysafe. This methodology will create the mostimportant security safety for any user, and that is awareness.By simply inputting a security scanner before savingonto a cloud activation and log-in for its users, can createmore viable software.Therefore, implementing various security checks uponregistering and giving the user options for its security toprovide easy to use functionality is of great importance.This password may be advanced, such as biometric scannerssuch as fingerprint scanners already used on mostmobile devices and is found to be a safe way to store dataon a device like a hard-drive.There are four levels in cloud security, and it isexplained in Table 1.Another method is to counter the ever-growingdemand for network access in both urban and rural areas,with rural areas being the most affected. Some peoplewant to access their information from a cloud almosteverywhere the need be, and network access can causemajor disruptions in a cloud functioning, for example, if the network cuts off, the document could not load ontothe cloud causing distortions in data and lack of it thereofstored in the cloud. To counter these problems, such aslack of network, this disrupts a server linking onto a cloudcomputing server because of a lack of network coverage, etc.This can cause a cloud to lose all of its information andsadly its stored data as a cloud server might depict a systemcrashing, (which can cause all stored data to delete,if the cloud user has not saved its data onto the cloudserver) the best way is if the service providers of a cloudand also its users work with each other to achieve ultimatesecurity. The best thing for a user is to report issuesregarding cloud to their service providers (cloud and alsotheir internet providers). The solution for network availabilityis simply the creation and viability of web to cloudservice providers. Web and service providers desired toexamine the control issues, techniques to prevent loss ofsignal, such as improve their coverage in areas that arehard to reach and provide more concise network signalcoverage in urban areas. This is done by getting the attentionof a user by giving the wrong impression and thenmaking the user aware of his mistakes. This will requirean advance algorithm from computer programmers, butit can be done. These advanced algorithms need to be constantly onthe run and updated by skilled programmers alike; thiswill keep intrusions on a cloud service hard to come by. These can go a long way in providing the safety a userwants and also the smooth process for service providersalike for a return in their investments. Figure 6illustrates the main uses of cloud computing areas. Figure 6. Main applied areas of cloud computing.

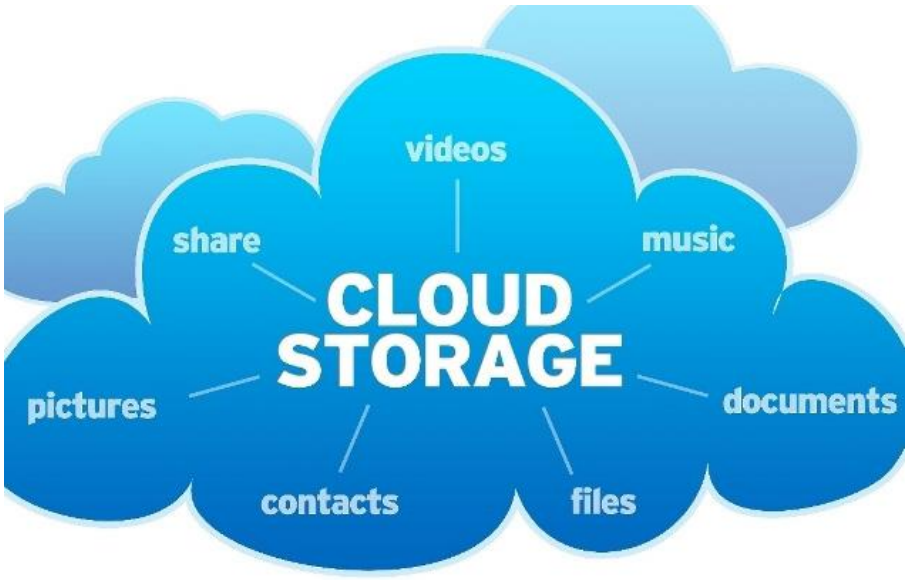

Figure 6. Main applied areas of cloud computing

3.1 Steps to Improve Cloud Security

• Make sure a user knows who's accessing whatand watching your every move: Every organization has a trusted IT administratorwho can make any changes regarding their computersystem or their clouds13.

• Users must limit their data access based on whata user is going to use it for:

A user must always be aware and continuously changingthe limit of accessibility of their data, depending onwhere the user is and what device they are using. Forexample: When a person uses a mobile device, he/she hasto go through additional sign-on steps and has more limitedaccess to the data14.

• The risk-based methodology is used to secure assetssuch as valuable information stored on a cloudand that's used in the cloud: Thus encrypt and provide extra protection for valuabledata.

• The use of extending security software to thedevice that is being used: Make guarantee that corporate data is secludedfrom personal data on mobile devices, such as tablets, smart-phones. Scan mobile applications from timeto time to check for security risk, and this can reduce toprevent loss of physical control, such as data loss and privacy15.

• Add artificial intelligence to network protection. The intelligence roll can be used in multiple ways, with its prime development being the protection of its network'sservice being provided to cloud operators. This willmake a user feels more secure in his attempts to use cloudcomputing properly16–19. As shown in Figure 7 illustrates the graph fromGoogle.com, showing that the increasing trends in cloudcomputing. Figure 7. Trends in cloud computing.

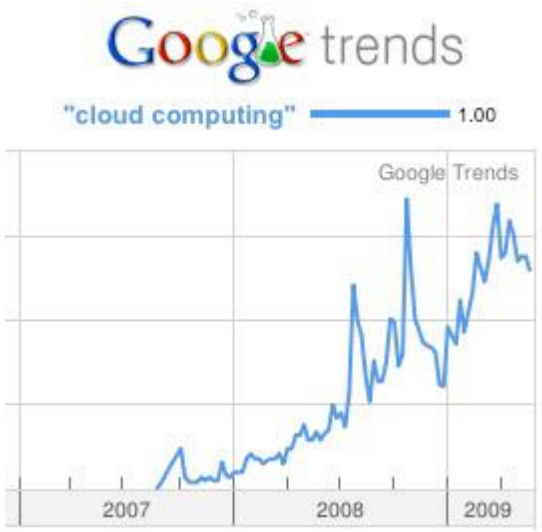

Figure 7. Trends in cloud computing

4. RESULTS AND DISCUSSION

The future development of cloud computing is to providea more precise service from cloud providers to its users. The results of security and cloud computing can go hand, hand, and can be a success, thus improving efficiency inthe growing field of the cloud computing industry as awhole. Thus this can improve its security issues anddevelop a more concise cloud computing product. The generic design principle of a cloud environmentis to control relevant security risks and threats. It needs asystemic point of view, from which protection of data ontrust, justifying security to a trusted third party20. Cloudsecurity concerns that impede the high rate adoption ofcloud computing. The cloud users are well knownabout the existing security threats in the cloud. This leads to minimal cost estimation in their security risk development. Earlier the cloud computing offers conventionaltechnologies and unique security issues. Currently, virtualizationallows various users (possibly from differentorigins) to utilize the same physical resource21.The discussion evolved on whether or not cloud providersand internet service providers will be willing toinvest their money into something that can take time toachieve. This result is also achieved by cloud and searchengine companies such as Google, who have taken thenecessary steps to improve their cloud computing serversand have been a success. They have implemented stepsto recover hacked cloud accounts and have taken precautionsagainst attacks in their cloud computing services. Itrequires co-operation of organizations, governments, andusers. This can be achieved, but it will take some time.Thus improve high reliability, efficiency, and create a senseof security in cloud computing22,23. Cloud computing isa recent innovative field, which came into existence afterlong research in networking and various types of computing.It utilizes an SOA that minimized the informationtechnology operating, and maintenance cost for the clientsgives greater flexibility, reduces capital costs, issuesrequired services are along with many other characteristics24.5. Conclusion and Future WorkThe projected methodology has a good ending and canbuild trust with many service providers. Trust is moreimperative and makes the triumph of cloud computing. Acloud offers a path to

(IJIASE) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

efficiency, reliability, security, andoffers very useful, easy to use control. Cloud computingcompanies are taking initiatives in improving securityissues, network issues, and providing a stable backgroundto smooth functionality. Organizations, industries, andusers should select their cloud providers with intensescrutiny and ensure they pick the best. This is to concernsthat the security risk concentrates on physical, software, and cloud security. As discussed throughout the area ofcloud computing, users have to be more aware thatthey are simply doing online and create a sense of safetyfor themselves, and this can be created using the cloudprovider's innovations. Ideas, innovations, and creativitycan go a long way to create an idea of ultimate safetyfor the providers and for the users as a whole. Currently, cloud computing is adopted by many corporate companiesand challenging the various issues like loadbalancing, network security, and green cloud computing, which have not been fully addressed. These are now beingaddressed by the concerned parties, and we look forwardto a safer, better, more advanced cloud computing inthe future. A more convenient way in cloud computingis needed, and this can take a while for it to be perfect inevery way. Certain cloud providers are taking huge stepsin dealing with cloud computing security issues and areplanning major developments for it to be extremely safeagainst attacks and error-free. This can be achieved, andwhen considering a move to use cloud computing, usersmust have complete knowledge of the potential securitybenefits, risks, and realistic expectations with their cloudprovider, for it to be extremely functional and safe. Theremust know consideration's as it's still in its development stage. Certain infrastructures such as IaaS, PaaS, and SaaS caneach play a major role in securing the future of cloud computing. This brings along additional security requirementsand responsibilities. This paper highlights the role users, service providers such as network and cloud computingplay in protecting and safeguarding cloud development. This can prove to be the future, and the future can be madesure of safety. However, this is a learning step to success.