IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 09 Issue 07, July 2022
ISSN (Online) 2348 – 7968 | Impact Factor – 6.72
www.ijiset.com

Usage of Trust Mechanisms in Cloud Computing Review

Mageto Stephen N [1], N.V.Balaji [2]
[1] Research scholar, [1] Karpagam Academy of Higher Education, Coimbatore, India.
[1] magetosteve@gmail.com
[2] Dean FASHA
[2] Karpagam Academy of Higher Education, Coimbatore, India.
[2] nvb1977@gmail.com

Abstract.
Cloud computing was developed by internet service providers to handle a high number of customers and elastic services. Over time, cloud computing has evolved into the most popular technology, with widespread adoption and use by a variety of businesses. As a result of this adoption, many businesses now store and analyze data in the cloud. This paper defines cloud computing, its architecture, and the trust mechanisms that assure cloud computing's confidentiality, integrity, and reputation.

Keywords: Security, Confidentiality, Trust, Integrity, Cloud Reputation.

1 Introduction

Cloud computing, as it's well known as "the cloud," is a modern processing technique that allows computers to process data through the internet. It's a form of computing that allows for scalability and elasticity. Customers get these functionalities through various internet-based services. Cloud computing, per the National Institute of Science and Technology, is a paradigm for providing on-demand network access to a shared pool of programmable resources that may be delivered and removed rapidly with minimal administration effort or involvement from service providers (NIST). Cloud computing creates a flexible online environment that allows for an increase in work volume without affecting the framework's implementation [1]. Cloud computing incorporates many of today's technologies in a web service-based infrastructure paradigm to provide business flexibility, increased scalability, simplified management, and on-demand resource availability. The end consumers don't need to know about the in-house technologies, hence this is a black box service. Cloud technology has a rapid deployment strategy, minimal startup investment, payment system, consumption, and sharing of shared resources, which are all elements that large enterprises use to convert their business applications into virtual apps [17]. Institutions can pay a usage charge to select Cloud Service Providers to receive the functionality of a system without having to buy hardware or software licenses or pay for maintenance. As a result, the cloud model is a significantly more cost-effective way to obtain and consume IT services [2].

The remainder of this work is divided into the following sections: characteristics of cloud computing, functional aspects of cloud computing, the architecture of cloud computing, security issues in cloud computing, application of cloud computing, research areas of cloud computing, research directions for the next generation in cloud computing, security aspect in cloud computing, usage of trust mechanisms in cloud computing, trust management, and finally trust-based access control.

2 characteristics of the cloud

Cloud computing features are explored in this section.

- **On-demand service;** The cloud is a massive collection of resources and services that you may access whenever you need them for a fee.
- **Ubiquitous network access;** Cloud services are accessible from anywhere using common terminals such as mobile phones, laptops, and personal digital assistants.
- **Simple to use**; the cloud provider offers web-based interfaces that are easier to use than application software interfaces, allowing customers to quickly access cloud services.
- **Business model;** Cloud is a business model since services or resources are paid for as they are used.
- **Location-independent resource pooling**; Pooling of resources regardless of location is utilized to serve numerous customers with varying physical and virtual needs using a multitenant architecture.

3 Functıonal aspects of cloud computıng

Users should ideally obtain their computing platform or IT infrastructure from the cloud and then run their apps within it. As a result, cloud computing gives consumers' transparent access to hardware, software, and data resources. The cloud offers three primary functions.

- **Software as a service (Saas)**.

  End-users are given software based on the services they have requested, which is often done through a browser. This prevents customers from having to deal with issues like software deployment and maintenance. The program is frequently shared by numerous tenants, receives automatic cloud updates, and does not require a separate license. The basic configuration is beyond the user's control. Features can be ordered on demand and sent out regularly. SaaS is frequently easy to combine with other applications due to its service characteristics. Google Maps[4] is an example of a SaaS product.

- **Platform as a service (Paas).**

  This service also called Cloudware is a development platform that includes a set of services for designing, developing, testing, deploying, monitoring, and hosting cloud applications. It usually does not necessitate any software downloads or installations, and it enables geographically distant teams to collaborate on projects.
  This layer includes Google App Engine, Microsoft Azure, and Amazon Map Reduce / Simple Storage Service [4]. Users of these services have no control over or access to the core physical infrastructure that their applications rely on.

- **Infrastructure as a service(Iaas)**

  The IaaS layer virtualizes computing power, storage, and connection in data centers and provides them to consumers as services. These computational resources can be dynamically increased and decreased on-demand by users. Multiple tenants usually share the same infrastructural resources.
  Amazon EC2 and Microsoft Azure Platform [4] are examples of this tier. The fundamental resources are under the entire control of the cloud service provider.

Table 1: Cloud computing service models are geared for different purposes.

Service model	Who uses it	Available services	Why use it
SaaS	Agency staff members	Software applications such as email, word processing and customer relation management tools	Complete business tasks that are typically performed locally on a computer
PaaS	Developers and application managers	Services for creating, testing, managing and hosting software applications	Establish a common and consistent platform for application development
IaaS	IT system managers	Virtual machines , storage services and backup services	Build a customized computing environment

4 Architecture of cloud computing

The cloud computing system can be divided into two parts: front end and back end [8]. They're both connected by a network, which is usually the Internet. The consumer (user) sees the front end and the rear end is the system cloud. The client computer and applications necessary to access the cloud are on the front end, whereas the back end contains cloud computing services such as computers, servers, and data storage. A central server is in charge of traffic monitoring, system administration, and customer requests. It adheres to particular guidelines, or protocols, and employs middleware programs. Middleware enables networked computers to communicate [4]. The infrastructure layer, platform layer, data center, and application layer are the four divisions of cloud computing's architectural design as shown in figure 1.

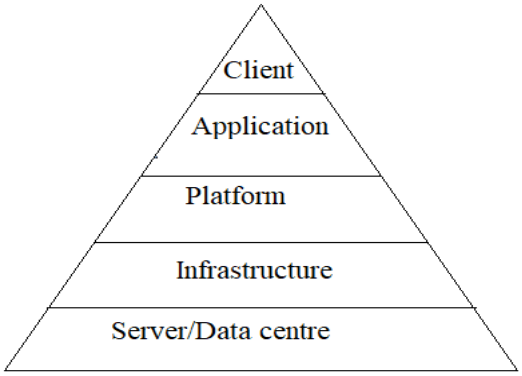


Figure 1: Different layers of cloud computing architecture.

a) ***The data center layer***. The data center, often known as the hardware layer, is in charge of handling and administering the cloud's physical resources. The router, power cooling systems, and physical servers are all part of this. Hundreds to thousands of servers are networked through routers and switches in the data center.

b) ***The infrastructure layer*** is the second layer. The physical resources of the data center are partitioned using virtualization to create a pool of computing and storage resources. This layer is critical because virtualization technology allows many cloud functionalities to be provided.

c) ***The platform layer***; On top of the infrastructure layer, this layer is set up. It includes both the operating system and the application framework. The platform layer is used to reduce the workload of deploying an application straight into a virtual machine container.

d) ***The application layer;*** The highest level of the hierarchy is this layer. It houses the real cloud application and is also the most visible to the user. The online portal or specific applications are used to access the services provided by this tier.

e) ***Cloud client:*** Comprises computers and/or computer programs that use cloud computing to provide applications or are specifically built to provide cloud services.

5 Securıty ıssues ın cloud computıng

Security is the main factor in storing sensitive information in the cloud. The user's details are sensitive information and high security should be provided. The following are the main security threats in storing and exchanging data in the cloud [28]

- **Access control**

  The unauthorized usage of sensitive information (Customer data) in the cloud can be prevented with the help of access control policies. Many organizations allow the users who have previously registered with their valid credentials can only access to the resources. The access control policies vary depending on their role. The access control policies outsourced in the cloud should not be leaked out.

- **Confidentiality**

  Confidentiality is the process of preserving the privacy of sensitive user information stored in the cloud unless the user grants permission to post it. It must be maintained by authorized persons and the cloud service provider. Users store data in encrypted form; We can convert plain text into ASCII code to ensure privacy. When sending data over the Internet, confidentiality must be maintained. When storing and retrieving data, key management issues have to be addressed.

- **Privacy**

  The authorized users can access their sensitive data at any time and can do any operations like read, write and update, etc and also determine how their sensitive data is shared with others. It involves maintaining confidentiality.

- **Authentication**

  Sensitive data should only be available to authorized users. The credentials provided by the users must match the credentials stored by the users in the authentication process. If credentials are disclosed, unauthorized users may have access to sensitive data for authorized users.

- **Availability**

  The sensitive data of cloud users stored in the cloud can be accessed by authorized users only at any time. Suppose if the resources are not available to the customers from another place, they cannot view the sensitive information. The unavailability may occur due to the poor internet connection and also that of information by the unauthorized

- **Data ownership**

  Most of the unauthorized users have access to sensitive information in bank data due to the lack of owner identity in the encrypted bank data. The use of encryption algorithms, by issuing public and private keys, makes them difficult for attackers to access

6 Applıcatıon of cloud computıng.

The following section discusses the application areas of cloud computing

a) Business and consumer applications.

Some of the many business management applications that are based on cloud computing are customer relationship management (CRM) and Enterprise resource planning (ERP). The method of deploying these services is software as a service. Cloud CRM applications create avenues for start-ups and small organizations to be wholly functional CRM software without huge costs and subscription fees. Salesforce.com is a well-known and well-developed CRM platform. This CRM provides customizable solutions that can be incorporated with features from a developed third party [1].

b) Big data analysis.

Cloud computing permits data scientists to attain organizational information that permits them to get insight, and forecast future decision-making based on the data. It won't be challenging to acquire and analyze data in rerealimeSome of the open-source data tools that are based on the cloud-like Hadoop, Cassandra, HPCC, and so on are used for small companies

c) Geoscience: Satellite Image Processing.

Satellite image processing applications are used to collect, produce and analyze a huge amount of nonspatial and geospatial data [1]. Cloud computing is an advancement for this kind of applicant for generating meaningful results. Satellite image sensing generates a lot of raw images. The processing of this data requires high computation power for both input and output. The large data can be transferred from the local station on the ground to cloud computing facilities for extra processing. Cloud computing provides accurate infrastructure for this kind of service.

c) Productivity.

Cloud-based applications are typically available through the web browser and can be operated anywhere and anytime through internet connectivity. Productivity applications in the cloud perform the similar task that we are used to doing on our desktops.

7 Research areas ın cloud computıng

The resources and services provided in the cloud have grown rapidly over the past decade. These changes have been supported by industry and academia efforts to realize computing as an aid. Applications increasingly try to take advantage of cloud infrastructure by combining resources from many providers. This contrasts with how the resources of a single cloud service provider or data center would be used traditionally. New computational architectures have evolved as a result. This shift has ramifications in a variety of cultural and scientific sectors [6]. Although cloud computing is widely adopted by the industry, cloud computing research is still in an early stage. Many of the current problems are not fully resolved, while new challenges arise from industrial applications. In this section, we summarize some of the challenging research questions in cloud computing [7].

- **Automated service provisioning**

One of the main characteristics of cloud computing is the ability to acquire and release resources on demand. In this situation, the service provider's purpose is to deploy and redeploy cloud resources to achieve service level goals (SLOs) while reducing operational costs. However, it is not clear how the service provider can achieve this goal. In particular, it is not easy to define how SLOs are assigned such as QoS requirements for low-level resource requirements such as CPU and memory requirements. In addition, to achieve high speed and respond to rapid fluctuations in demand, such as the effect of rapid crowding, resource-saving decisions must be made online. Automated servicing is not a new problem. These methods typically include the following: (i) Building an application performance model that predicts the number of application instances needed to handle the demand at each

particular level, to meet QoS requirements; (ii) Periodic forecasting of future demand and determination of resource requirements using the performance model; And (iii) Automatic resource allocation using planned resource requirements.

- **Virtual machine migration**

Virtualization can help in cloud computing by allowing virtual machines to migrate to balance the load in the data center. In addition, virtual machine migration allows data centers to save money while remaining stable and responsive. Virtual machine migration has evolved from process migration technologies. More recently, Xen and VMWare implemented a "live" relay of virtual machines that involved an extremely short downtime ranging from tens of milliseconds to a second.

Clark et al. [13] point out that migrating the complete operating system and all of its applications to a single unit avoids many of the challenges of process-level migration strategies, and they go on to describe the advantages of direct migration for virtual machines. The main advantages of migrating virtual machines are to avoid hotspots; However, it is not easy. Currently, discovering workload hotspots and initiating migration cannot respond to sudden changes in workload. Additionally, the state should be moved in memory consistently and efficiently, with in-built consideration for application resources, physical servers, and servers.

- **Server consolidation**

Server consolidation is an effective way to optimize resource usage while reducing energy consumption in a cloud computing environment. VM Live Migration technology is often used to consolidate virtual machines across multiple underutilized servers into one. This allows you to install the rest of the servers if they are powered. Datacenter server optimization problems are often formulated as variants of the NP-hard optimization problem, and the container-filled bus problem. Various heuristics have been proposed on this issue. In addition, dependencies between virtual machines, such as connection requirements, have recently been considered. However, server consolidation activity does not adversely affect application performance. It is well known that the resource usage of individual virtual machines can change over time. For server resources shared between virtual machines, such as bandwidth, memory cache, and disk I / O, maximizing server consolidation causes resource congestion when the virtual machine changes its impact on the server. There is a possibility. Therefore, it may be important to be aware of fluctuations in the virtual machine footprint and use this information to effectively consolidate your servers. Finally, the system needs to respond quickly when resource congestion occurs.

- **Energy management**

Improving energy efficiency is another major challenge of cloud computing. Energy and cooling cost was estimated by accounting for 53% of total data center operating expenses.

In 2006, data centers in the United States consumed more than 1.5% of the total energy produced that year, and the proportion is expected to increase by 18% annually. As a result, infrastructure providers are under a lot of pressure to cut down on their energy usage. The goal is not only to reduce energy costs in data centers but also to meet government regulations and environmental standards. The design of energy-efficient data centers has received much attention recently. This problem can be dealt with in several directions. For example, energy-efficient hardware architecture that allows slow down processor speeds and partial hardware component disruption is becoming commonplace. Energy-based task scheduling and server consolidation are two other ways to reduce power consumption by shutting down unused devices.

Energy-efficient network protocols and infrastructure have been the subject of recent research. The main challenge with all of the above approaches is to achieve a good compromise between energy savings and application performance. İn this regard academics have lately started to examine coordinated solutions for performance and energy management in a dynamic cloud environment

- **Traffic management and analysis**

Traffic analysis is important to today's data centers. For example, many web applications rely on analyzing traffic data to improve the customer experience. Network operators also need to know how network traffic flows to make many management and planning decisions.

However, there are many challenges facing current traffic measurement and analysis methods in networks of Internet Service Providers (ISPs) and companies for expanding into data centers. First, the link density is much higher than that of ISPs or corporate networks, which is the worst-case scenario for current methods. Second, most current methods can compute matrices of traffic between a few hundred ultimate hosts, but even a standard data center can have several thousand servers. Finally, current methods generally assume reasonable flow patterns in Internet and corporate networks, but applications deployed in data centers, such as MapReduce change the traffic pattern significantly. In addition, there is a closer association in network resource use, computing, and storage by applications than has been observed in other contexts.

Currently, there isn't much work being done on measuring and analyzing data center traffic.

- ***Data security.***

Security is another important research topic in cloud computing. Since service providers usually do not have access to a data center's physical security system, they must rely on the infrastructure provider to ensure complete data security. Even for a virtual private cloud, a service provider can only define the security setting remotely, without knowing whether or not it's fully implemented. In this context, the infrastructure provider should achieve the following objectives: (1) confidentiality, for secure access and data transfer, and (2) auditing, to validate whether or not the application security setting has been tampered with. Confidentiality is usually achieved using encryption protocols, while auditing can be achieved using remote authentication techniques. Remote authentication usually requires the Trusted Platform Module (TPM) to create a tamper-proof system summary (i.e. the system state encrypted with the TPM's private key) as evidence of the system's security. However, in a virtual environment such as a cloud, virtual machines can migrate dynamically from one location to another; Therefore, direct use of remote authentication is not sufficient. In this case, it is imperative to establish trust mechanisms at the level of each cloud architectural layer. First, the hardware layer must be trusted with the device TPM. Second, the virtualization platform must be trusted with secure virtual machine monitors. Virtual machine migration should only be authorized when both source and destination servers are trusted. Recent work is devoted to designing effective protocols for building and managing trust.

- **Software frameworks**

Cloud computing provides a compelling platform for hosting large-scale data-intensive applications. Typically, these applications take advantage of MapReduce frameworks like Hadoop for scalable and fault-tolerant data handling. According to recent research, MapReduce's performance and resource consumption are largely depending on the type of application. For example, Hadoop tasks like sorting are I / O hungry, while grep requires large CPU resources. Additionally, a VM assigned to each Hadoop node can have heterogeneous properties. For example, the available bandwidth for a virtual machine depends on other virtual machines on the same server. Therefore, it is possible to improve the performance and cost of the MapReduce application by carefully determining the values of configuration parameters and designing more efficient scheduling algorithms. By mitigating throttle resources, application uptime can be greatly improved. Key challenges include Hadoop functionality modeling (online or offline) and adaptive planning under dynamic conditions.

8 Research dırectıons for the next generatıon cloud computıng.

In light of the new trends discussed in the preceding parts, this section outlines a few avenues in which academicians in cloud computing research can contribute.

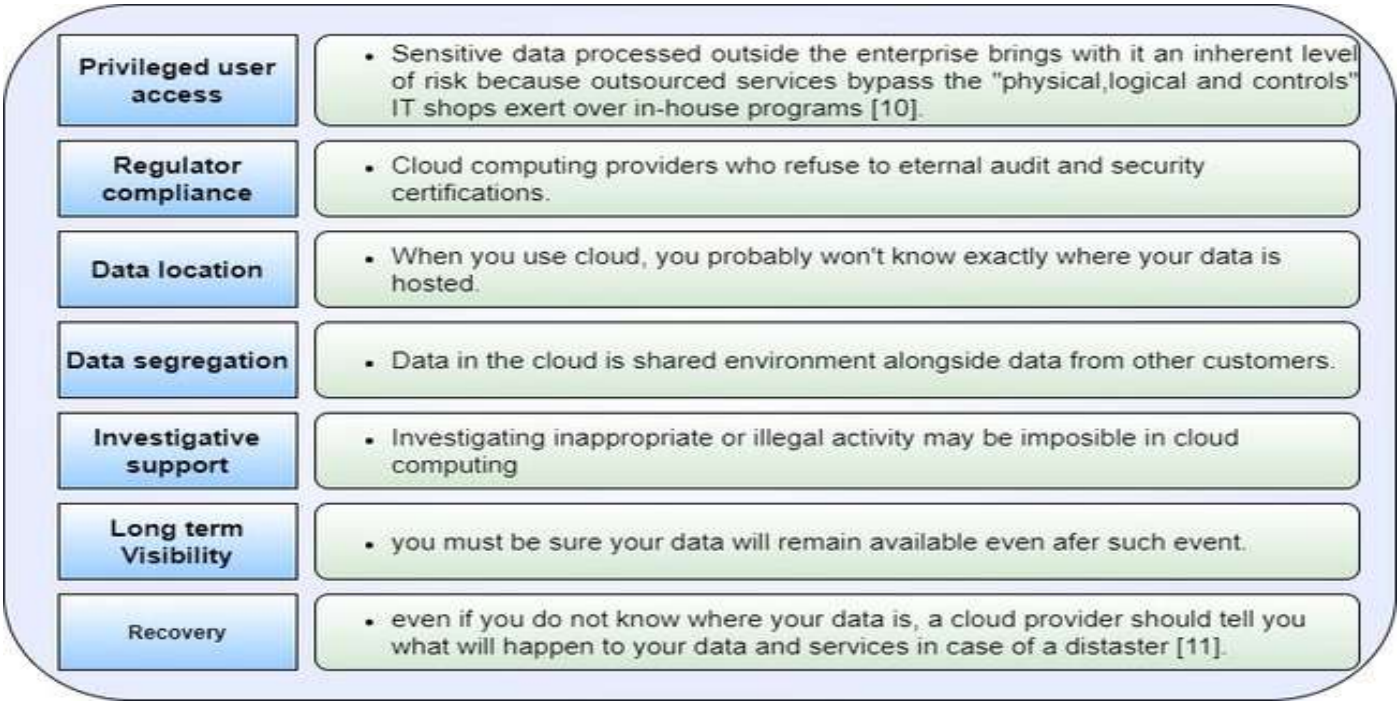
Table 2: *Research dırectıons for the next generation cloud computıng*

Research Directions for the Next Generation Cloud Computing	
Sustainability	• Carbon footprinting aware and energy aware provisioning in datacenters and understanding trade off between energy and virtualized network
Security	• Point to Point encryption - decryption mechanisms • Security for computing and data on edge nodes
Reliability	• Developing low cost operations • Accounting for distributed cloud resources
Market place	• Accounting for distributed ownership • Developing industry academic collaboration
Expresivity	• Serverless computing for distributed clouds • Miniaturizaing algorithms for resource constrained environment
Management	• Virtical scaling mechanisms • Lightwaight monitoring, brokerage and benchmarking

9 *Security aspect in cloud computing.*

The cloud computing model is gaining popularity in industry and academia. Cost-effective, scalable, fast, comprehensive, and on-demand access to shared resources are some of the characteristics of the cloud that have led to the migration of cloud-based business processes [8] to improve work efficiency, different departments are distributed on different servers distributed in different places. One of the major obstacles to the widespread adoption of cloud computing is security. Hence, security is a key component of any cloud computing infrastructure, as it is necessary to ensure that only authorized access is allowed and that secure behavior is acceptable. In short, all members of the cloud and the cloud computing environment must trust each other, and the members who communicate must trust each other [9 A traditional computing infrastructure either in nature, in density, or both allows the pooling of resources to use the same group by multiple users thanks to exchange and virtualization technologies. Multiple leases run the risk of seeing data for other users and keeping track of operations.

Table 3: Seven cloud-computing security risks



9.1 Security at Different Levels.

Various levels of security concerns in cloud computing

Table 4: Security in Clouds: Levels and Concerns

Network security	- **Secure data transmission** - **Data sharing with authorized users** - **Transparent security protocol**
Privacy	- Data location privacy - Cryptography technique for data security - Hidden and redundant backup of data
Virtual machine security	- Virtual machine management - Virtualization - Virtual machine identification
Compliance	- Standardized service level - Audit

	- Trust management among participants
Interface security	- Secure user interface
	- Robust administrative interface
	- Secure application programming interface

Description of various security concerns are as follows;

- **Network Security**

When information travels across the network, network security becomes a concern. Cloud service providers must ensure the adoption of a robust and secure communication protocol to prevent attacks on information as it travels across the network.

- **Interface Security**

It is directly affected by the interface that cloud providers provide and the level of security that they provide. The VM interface affects inherent security features such as IBM Blue Mix, a Linux-based cloud service, and Microsoft Azure-based on the Windows operating system.

Linux is more secure than Microsoft Windows. So interface security would be better with the Linux interface. Hence, the interface provided by the CSP has to publish a secure operating system

- **Virtual Machine Security**

The security of virtual machines is the biggest concern among all security concerns. Users use the VM for their processing tasks. In addition, the cloud uses multi-rental technology, that is the same virtual resources and the same resources are used by different users at different times to optimize resource utilization and reduce costs. However, this increases the possibility of security breaches. Multiple users of the same virtual machine should be isolated as an individual can be kept confidential.

- **Compliance**

Compliance focuses on implementing the Said Service Level Agreement (SLA). A service level agreement is the only legal document between a user and a service provider that defines the user's service requirements and service standards that the provider will provide. However, there is no standardization of SLAs which is necessary to make this business model trustworthy. Improper implementation of service standards by the provider can lead to security breaches.

- **Privacy/Confidentiality**

Privacy focuses on preventing private information from being disclosed to unauthorized users. In cloud computing, all data is stored in geographically separate locations, thus ensuring data privacy becomes a major problem. A typical solution adopted is the application of various encryption algorithms. Data segmentation is another method used to ensure data security on the vendor's side. In this technique, data is stored on multiple hosts that do not interact. However, the two methods mentioned above have inherent problems of them [18].

10 Usage of trust mechanısms ın cloud computıng

In a cloud computing environment, many users join or leave the cloud dynamically. The same is true for other resources in a cloud computing environment. Users, resources, and the cloud need to build trust with each other. This will also allow handling changes dynamically. The cloud consists of distributed users and resources from local distributed systems or organizations, which have different security policies. Building an appropriate relationship between them is a challenge. There are some aspects of the security requirements of a cloud computing environment, including privacy multiple security policies, and dynamic services. Trust between entities and building areas of trust dynamically [9]. Security and interoperability are currently the biggest challenges in enhancing cloud computing. Trust has proven to be one of the most important and effective alternative ways to build security in distributed systems to build entities efficiently, securely, trust, and relationships in the cloud environment and across the cloud [12].

10.1 What Is Trust?

Trust means an act of faith, confidence in something that should act or deliver as promised. It is a belief in the skill and expertise of others so that you feel you can be reasonably relied upon to take care of your valuable possessions. (13) thus we can say Trust is referred to the recognition of an entity’s identity and the confidence in its behaviors.

10.2 Classification of Trust.

Trust can be classified into different categories according to different standards.

- Based on characteristics: identity trust and conduct trust.
- According to the method of getting trust: are direct trust and suggested trust.

- According to the role: code trust, third-party trust, and execution trust.
- According to the underlying theory: subjective trust and objective trust.

11 Definition of different Trust relationships

A trust relationship can be one-to-one between two entities; however, it may not be symmetric. A's trust in B is not usually the same as B's trust in A. It may be a one-to-many relationship in that it can apply to a group of entities such as the set of students in a particular year. It can also be many-to-many such as the mutual trust between members of a group or a committee, or many-to-one such as several departments trusting a corporate head branch [20]

Table 3: Definition of different trust relationships

Trust Degree	Represent the tendency which entity the user would choose to interact
Direct Trust	Direct trust relationship is built through direct experience of interaction between the user and entity.
Trust Pheromone	Trust pheromone formalized as T_p is primary cognition of direct trust degree between the user and the entity.
Heuristic Pheromone	Heuristic pheromone formalized as H_p is user's cognitive information about the server node.
Recommend Trust	Recommend trust or R_t is recommended by some intermediate entity.
Mutual Trust	Mutual trust is the confidence that both user and cloud service nodes have shown each other in the face of uncertainty in the future interactions.
Mutual Trust Threshold	Mutual trust threshold (MTT) is composed of binary group $MTT=< TT_{user}, TT_{cloud} >$. TT_{user} is user's trust threshold and TT_{cloud} is trust threshold of cloud service node.
Trust Decision	Trust decision can be formalized as T_d, $T_d \in \{0,1\}$

11.1 Some of the proposed models are based on the trust model on the distributed system

a) Public key infrastructure-based trust model

This trust model relies on a few leading nodes to secure the entire system. Certificates of authority for officers are signed by the CA because it places too much reliance on the primary nodes, the PKI architecture can result in an unequal load or a single point of failure.

b) Network topology-base trust model

This trust model is built on the network architecture. Each entity's trust is evaluated based on its position in the system's topology and usually uses a tree or graph traversal algorithm. The trust management mechanism in this model is relatively straightforward. However, due to the high complexity of the network environment, trust values are often imprecise, which can lead to security risks in the system

c) Behavior-based trust model:-

This model uses history trade records to compute trust. One entity's trust is gained by considering both former trade experiences and other nodes' recommendations. Trust value is relatively complete and reliable in this model while at the same time with large-scale computation and other burdens

d) Subjective trust model

Distributed applications often encounter two main security scenarios. First, user programs can contain malicious code that can compromise or weaken resources. Second, once affected by network attacks, resources can damage users' applications. Thus, the model of trust based on subject logic divides trust into several subcategories: execution trust, code trust, authority trust, direct trust, recommendation trust, etc. Additionally, he designs different strategies for each type of trust. Self-confidence is a personal decision about a certain level of personality or behaviors of an entity. Entity (i) trusts Entity (ii) means that (iii) believes that (iv) will perform certain actions in a given situation. Probability theory, for example, D-S theory or fuzzy mathematics, is the primary tool for determining confidence. But in general, self-confidence cannot reflect ambiguity and causes only around likelihood models that are too formal and far from the true essence of trust management. The literature [9] has proposed a new model of self-confidence based on the cloud model that can better describe ambiguity and randomness. There are other shortcomings such as that it is not possible to achieve the integrity of the certificate of identity, and behavior and the mechanism is so complex that it is difficult to achieve the system based on it.

e) Domain-based trust model.

This trust model is mainly used in grid computing. It divides the network environment into several domains of trust and distinguishes between two types of trust. One is the relationship of trust in the domain and the other is the relationship of trust between domains. İt sets various strategies for them. The mechanism of this model is reasonable in that because nodes in the same domain are generally more familiar, they generally have a higher degree of trust in each other. This algorithm is of low computational complexity because the calculation of trust in the domain depends only on the number of nodes in the domain and the trust between the domain depends only on the number of domains. The domain-based model can be thought of as a compromise between the PKI and the network topology. But like Public Key Infrastructure (PKI), it can cause network bottleneck and a single point of failure, and ignore the decision to trust the independence of entities.

f) Dynamic Trust Model

The dynamic trust mechanism is a hot new topic in the security research of distributed applications. Building a dynamic trust relationship should solve the following mathematical problems.

- To decide trust degree space. Always it is defined by fuzzy logic.
- To design a mechanism of acquirement of trust value. There are two kinds of methods: direct and indirect.
- To design a mechanism of trust value evaluation or evolution.

12 Trust management

Trust mechanism can establish entities' relationship quickly and safely in distributed systems and has been proven to be an effective substitute means for traditional security mechanisms. However trust is extremely abstract, subjective, uncertainty, time and context-sensitive, and it is very difficult to be measured and managed.

Trust management systems allow trusted parties/entities to reliably represent their capabilities and competencies of the underlying systems in terms of relevant attributes. A cloud computing trust management system must be able to combine trust based on multiple attributes derived from multiple sources and roots: soft (such as user comments or reviews) and company trust (such as testimonials or audits) [14]. The trust model consists of methods or protocols for managing the trust, including building trust, renewing trust, and removing trust. Several types of trust models are designed for distributed systems, such as the PKI-based trust model, the network topology-based trust model, the behavior-based trust model, the self-trust model, and the domain-based trust model.

Even today, with the rapid adoption of cloud computing in the industry, trust management remains one of the key challenges in adopting cloud computing. In fact, according to researchers at the University of California, Berkeley, [Armbrust et al. 2010], One of the top ten barriers to cloud computing adoption is trust and security. This is due to complex issues such as privacy, security, and reliability. Trust is one of the most troubling obstacles to cloud computing adoption and growth. Several solutions have recently been proposed for managing trust returns in cloud environments, but there are ways in which trust in trust returns is largely overlooked. Due to the unexpected number of consumers of cloud services and the highly dynamic nature of cloud environments, managing trust returns in cloud environments is also a difficult problem

Effective trust management systems help cloud service providers and consumers enjoy the benefits of cloud computing technology. Despite the benefits of managing the trust, many issues related to public trust assessment mechanisms, suspicious comments, misidentification of comments, participant confidentiality, and comment incompleteness still need to be addressed. Traditional methods of managing the trust, such as using a Service Level Agreement (SLA), are not suitable for complex cloud environments. Ambiguous terms and unclear technical specifications of SLAs can lead consumers of Cloud services to be unable to define reliable Cloud services [14].

To improve approaches to trust management in cloud environments, Talal H. Noor et al suggested trust as a service paradigm. As part of that, they introduced an adaptive reliability model that distinguishes between trusted and malicious comments, taking into account the capabilities of cloud users and the comments of the majority of opinions [19]. Ruohomaa et al [2005] present several trust models. They identify trust actors and categorize trust management into three tasks. This includes (i) establishing relationships of trust, (ii) monitoring behavior, and (iii) behavior after new experiences.

12.1 Trust Management Techniques

Different trust management techniques have been reported in the literature, which can be classified into four different categories: Policy, Recommendation, Reputation, and Prediction.

- **Policy as a Trust Management Technique**

Policy as a trust management technique is one of the most popular and traditional ways to establish trust among parties and has been used in cloud environments, the grid, P2P systems, Web applications, and the service-oriented environment. Policy as a The Trust Management Technique employs a series of policies, each of which serves a variety of functions in controlling permission levels and defining a minimum trust threshold for granting access. The trust thresholds are determined by the results of the trust test or the credentials.

- **Recommendation as a Trust Management Technique.**

Recommendation as a trust management technique has been widely used in the cloud environment, the grid, and the service-oriented environment. Recommendations take advantage of participants' knowledge about the trusted parties, especially given that the party at least knows the source of the trust feedback. It is well known in social psychology theory that the role of a person has a considerable influence on another person's trust assessment if a recommendation is given [21]. Recommendations can appear in different forms such as the explicit recommendation or the transitive recommendation. An explicit recommendation happens when a cloud service consumer recommends a certain cloud service to her well-established and trusted relations (e.g., friends). A transitive recommendation happens, on the other hand, when a cloud service consumer trusts a certain cloud service because at least one of her trusted relations trusts the service.

- **Reputation as a Trust Management Technique.**

Reputation as a trust management technique is important because the feedback of different cloud service users can drastically determine the reputation of a given cloud service, either positively or negatively. Unlike Recommendation as a Trust Management Technique, in Reputation as a Trust Management Technique, cloud service consumers do not know the source of the trust feedback, because there are no trusted relations in Reputation as a Trust Management Technique.

- **Prediction as a Trust Management Technique.**

Prediction as a trust management technique is very useful, especially when there is no prior information regarding the cloud service's interactions (e.g., previous interactions, history records). The basic idea behind prediction as a trust management technique (PrdT) is that similar-minded entities (e.g., cloud service consumers) are more likely to trust each other

13 Trust-based access control

Access control needs to be provided at different granularity levels in the cloud. Different types of protection are expected from the access control services

1. In the Software as a service model, the major service is the protection of user data.
2. In the Platform as a service model, the major service is the protection of tenant resources.
3. In Infrastructure, as a service model, the major service is the isolation of the provider's resources from tenants

Access control is the key technology to meet the security requirements of cloud computing. Access control takes charge of the authentication, the control, and the management of resources. It's one of the security measures in a multi-user shared resource environment. If any user wanted to access any cloud service then his request will pass through several modules before completing the authorization process. The resource catalog contains several resources which have different reputations and trust values in the cloud environment. When a user requests a resource trust-based access control model checks whether the requesting user is a trusted user or not. If the user is found as a trusted user then the best resource for the requesting user is provided from the mutual trust relationship and his computational needs.

The mutual trust mechanism of users and cloud service nodes has a two-part structure. One part is the trust evaluation model of users' behavior and the other part is the trust computation model for cloud service nodes.

13.1 Related work on trust-based access control

Access control takes charge of the authentication, the control, and the management of resources. It's one of the security measures in a multi-user shared resource environment. Role-based access control (RBAC) models have gained a great interest in the security community and figured out the localization and disadvantage of discretionary access control (DAC) and mandatory access control (MAC) to some extent. Subsequently, Osborn et.al and Ang et.al have proposed many extensions that expand the description and adaptation range of RBAC[23,24]. In a distributed environment, the dynamic and randomicity of users' behaviors make it more and more difficult to control the resources and bring more security problems to the system.

Riaz et al. Proposed a multi-factor integration of trust-based access control decision-making that provides the basis for granting access based on three elements that examine key metrics in a cloud environment and their semantic relationships. This model supports dynamic changes in permissions assigned to users based on trust level and also ensures secure sharing of resources between potentially untrusted tenants [25].

Banyal et.al . proposed a framework based on the dynamic trustworthiness of users and provide an effective and feasible access control solution for the cloud where multilayer security standards, policies, and access control mechanisms are provided. The access control is based on the trustworthiness of the user which is demonstrated by static and dynamic trust evidence. In this framework, dynamic trustworthiness is used to reduce the possibility to perform unauthorized activities and ensure that only authorized users access the cloud [26].

Zhau et.al proposed a model that integrates trust with cryptographic bole-based access control for secure cloud data storage. When evaluating trustworthiness roles, this model considers role inheritance and hierarchy [27].

14 Trust Characteristics in Cloud Services

Many researchers use a qualitative approach to compare existing cloud services for all three different service models (i.e., IaaS, PaaS, and SaaS) among several cloud service providers from different perspectives such as the security features, virtual infrastructure management capabilities, and services functionalities. On the other hand, others use a quantitative approach to compare the use of cloud services among several cloud service providers (i.e., in terms of the number of cloud service consumers). In the following, we define a set of trust characteristics authentication, security, privacy responsibility, virtualization, and cloud service consumer accessibility.

- **Authentication.** This characteristic refers to the techniques and mechanisms that are used for authentication in a particular cloud. Cloud consumers have to establish their identities every time they attempt to use a new cloud service by registering their credentials, which contain sensitive information. This can lead to privacy breaches if no proper identity scheme is applied for the cloud service consumers.
- **Security.** There are three security levels in a particular cloud: the Communication Security Level (CSL), the Data Security Level (DSL), and the Physical Security Level (PSL). CSL refers to communication techniques such as Secure Socket Layer (SSL), etc. DSL refers to data replication techniques for data recovery. Finally, PSL refers to physical security techniques such as hardware security. —Privacy Responsibility. Privacy responsibility can be categorized into two different privacy responsibility categories: the cloud service provider privacy responsibility category and the cloud service consumer privacy responsibility category.
- **Virtualization.** This characteristic refers to techniques that are used for virtualization. There are two virtualization levels in a particular cloud: the Operating System (OS) level and the application container level. Virtualization techniques allow the cloud service provider to control and manage the underlying cloud environment, whereas the cloud service consumers have control over their virtual machines which include the storage, the process, and even the selection of some network components for communication.
- **Cloud Consumer Accessibility.** This characteristic refers to techniques and mechanisms that are used for cloud service consumers to access cloud services such as Graphical User Interfaces (GUIs), Application Programming Interfaces (APIs), command-line tools, etc[22]

Conclusion

Cloud computing is the on-demand utilization of shared computing resources available from the Internet. When these services are used properly, they can reduce cost and management responsibilities in addition to increasing the efficiency, agility, and performance of an enterprise. On the contrary, there are several challenges to be faced by cloud computing such as data security and privacy issues. In this paper, we looked at how trust may be utilized to solve

security problems by quickly and safely establishing relationships between entities. We examined some of the existing research and practices of trust mechanisms for cloud computing.

Reference

[1]. Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: a perspective study. *New Generation Computing*, *28*(2), 137-146.

[2]. Thomas, P. Y. (2011). Cloud computing. *The Electronic Library*.

[3]. Adrian voss, 2010. Cloud computing it's a journey https://www.itapa.sk/data/att/628.pdf

[4]. Tsai, W. T., Sun, X., & Balasooriya, J. (2010, April). Service-oriented cloud computing architecture. In *2010 seventh international conference on information technology: new generations* (pp. 684-689). IEEE.

[5]. Jadeja, Y., & Modi, K. (2012, March). Cloud computing-concepts, architecture and challenges. In *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)* (pp. 877-880). IEEE.

[6]. Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849-861.

[7]. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.

[8]. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

[9]. Shen, Z., & Tong, Q. (2010, July). The security of cloud computing system enabled by trusted computing technology. In *2010 2nd International Conference on Signal Processing Systems* (Vol. 2, pp. V2-11). IEEE.

[10]. Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. *Infoworld*, *2008*, 1-3.

[11]. Gampala, V., Inuganti, S., & Muppidi, S. (2012). Data security in cloud computing with elliptic curve cryptography. *International Journal of Soft Computing and Engineering (IJSCE)*, *2*(3), 138-141.

[12]. Li, W., Ping, L., & Pan, X. (2010, August). Use trust management module to achieve effective security mechanisms in cloud environment. In *2010 International Conference on Electronics and Information Engineering* (Vol. 1, pp. V1-14). IEEE.

[13]. Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT professional*, *12*(5), 20-27.

[14]. Habib, S. M., Ries, S., & Muhlhauser, M. (2011, November). Towards a trust management system for cloud computing. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 933-939). IEEE.

[15]. Khilar, P. M., Chaudhari, V., & Swain, R. R. (2019). Trust-based access control in cloud computing using machine learning. In *Cloud Computing for Geospatial Big Data Analytics* (pp. 55-79). Springer, Cham.

[16]. Li, W., & Ping, L. (2009, December). Trust model to enhance security and interoperability of cloud environment. In *IEEE International Conference on Cloud Computing* (pp. 69-79). Springer, Berlin, Heidelberg.

[17]. Aruna, E., Shri, A. A., & Lakkshmanan, A. (2013, December). Security concerns and risk at different levels in Cloud Computing. In *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)* (pp. 743-746). IEEE.

[18]. Singh, A., & Malhotra, M. (2015). Security concerns at various levels of cloud computing paradigm: A review. *International journal of computer networks and applications*, *2*(2), 41-45.

[19]. Noor, T. H., & Sheng, Q. Z. (2011, October). Trust as a service: A framework for trust management in cloud environments. In *International conference on web information systems engineering* (pp. 314-321). Springer, Berlin, Heidelberg.

[20]. Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, *3*(4), 2-16.

[21]. Liu, G., Wang, Y., & Orgun, M. (2009, August). Trust inference in complex trust-oriented social networks. In *2009 International Conference on Computational Science and Engineering* (Vol. 4, pp. 996-1001). IEEE.

[22]. Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys (CSUR)*, *46*(1), 1-30.

[23]. Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security (TISSEC)*, *3*(2), 85-106.

[24]. Ahn, G. J., & Sandhu, R. (2000). Role-based authorization constraints specification. *ACM Transactions on Information and System Security (TISSEC)*, *3*(4), 207-226.

[25]. Riad, K., & Yan, Z. (2017). Multi-factor synthesis decision-making for trust-based access control on cloud. *International Journal of Cooperative Information Systems*, *26*(04), 1750003.

[26]. Banyal, R. K., Jain, V. K., & Jain, P. (2014, October). Dynamic trust based access control framework for securing multi-cloud environment. In *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies* (pp. 1-8).

[27]. Zhou, L., Varadharajan, V., & Hitchens, M. (2013, July). Integrating trust with cryptographic role-based access control for secure cloud data storage. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 560-569). IEEE.

[28]. Suveetha, K., & Manju, T. (2016). Ensuring confidentiality of cloud data using homomorphic encryption. *Indian Journal of Science and Technology*, *9*(8), 1-7.

[29]. R. Kerr and R. Cohen, "Smart cheaters do prosper: defeating trust and reputation systems," in AAMAS '09: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems. Richland, SC: IFAAMAS, 2009, pp. 993– 1000.

[30]. G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in Proceedings of the ACM SAC, 2011.

[31]. Banyal, R.K.; Jain, P.; Jain, V.K., "Multi-factor Authentication Framework for Cloud Computing," Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on , vol., no., pp.105,110,24-25,Sept.2013, doi: 10.1109/CIMSim.2013.25

[32]. H. Takabi, J. B. D. Joshi, and G.J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments" in Proc. of the 1st IEEE International Workshop Emerging Applications for Cloud Computing (CloudApp 2010), pp. 393-398, Seoul, South Korea,(2010).

[33]. Chunming Rong, Son T. Nguyen, Martin Gilje Jaatun, "Beyond lightning: A survey on security challenges in cloud computing" Computers and Electrical Engineering 39 (2013) 47-54