A Revolutionary Approach to Cloud Computing, Security and its User Compliance

M. R. Sudha* and M. Sornam2

1Department of Computer Science, Faculty of Science and Humanities, SRM University, Kattankulathur - 603203, Tamil Nadu, India; sudha.mr@ktr.srmuniv.ac.in
2Department of Computer Science, University of Madras, Chepauk Campus, Chennai - 600005, Tamil Nadu, India; madasamy.sornam@gmail.com

Abstract

Objective: This paper focus on the ways to initiate service providers to create safer clouds by simply securing cloud computing servers, inputting a security scanner before saving onto a cloud and finally before accessing a cloud, the use of a password or key to enter your cloud account. Methods: This paper is an extensive research in the cloud security through password might be advanced such as bio-metric scanners, finger-print scanners already used on most mobile devices and is found to be a safe way to store data on a device like a hard-drive. The major complexity of cloud computing is security privacy. Security compliances are like protection of data, and check the usage and applicability of cloud computing providers. Findings: The main theme of cloud computing has various courageous for the users and this facility providers regarding security. To counter these problems, such as lack of network, this disrupts a server linking onto a cloud computing server because of lack of network coverage etc. This can cause a cloud to lose all of its information and sadly its stored data as a cloud server might depict a system crashing, (which can cause all stored data to delete, if the cloud user has not saved its data onto the cloud server) the best way is if the service providers of a cloud and also its users work with each other to achieve ultimate security. The best thing for a user is to report issues regarding cloud to their service providers (cloud and also their internet providers). The solution for network availability is simply the creation and viability of web facility to cloud users. Improvements: Web users and data facility providers require to examine the way to control issues and apply various techniques to prevent loss of signal, such as improve their coverage in areas hard to reach and provide more concise network signal coverage in urban areas. In fact, a signal enhancer has been hard to reach areas such as rural areas. This requires an advanced algorithm from computer programmers.

Keywords: Algorithms, Cloud Computing, Cloud Services, Cloud Security, Hacking

1. Introduction

Cloud computing is merely to put the stored information onto a server via the use of the internet. Nowadays, this has become the norm; many people around the world, either young or old use this to their advantage. Let’s not forget about the power of massive industries that use clouds to store data and sensitive information. This can be used to basically do about anything on any device throughout the world as long as you have a user-name and password.

The basic idea is that cloud computing, falls under a sort of web based computing, in which we can share resources, data and information. A cloud computing provider has various capabilities to store and process data. Cloud service providers are demand by the pay for accessing the cloud services. Consumers, such as enterprises, are attracted by the opportunity for reducing or eliminating costs associated with “in-house” provision of these services. Typically, these are provided through Service Level Agreements (SLAs) brokered between the providers and consumers. Providers like Amazon, Google, Sales force, IBM, Microsoft, and Sun Microsystems have started to develop new data centers for hosting cloud computing applications in various locations around the world to
provide redundancy and make certain consistency. As the demands of user for cloud services are varied, service providers have to ensure that the flexibility in the service delivery while keeping the users isolated from the essential infrastructure\(^1\). Cloud providers are reuse the resources after relinquish by the particular user resulting in high resource utilization\(^2\). User friendly environment is another advantage of cloud computing because it does not require the customers to possess astonishing knowledge pertaining to the cloud technologies\(^3\). Cloud computing has behaviour to earlier routes of the internet with the idea from the American military to store its digital data and sensitive information online, which back then was a major development because of the cold war and against Russia. That could be seen as a step to a safer way of securing data, however back then only a small amount of data was used compared to the massive Terabytes we can harness now days. This lead to the massive development of cloud computing from the 1960’s to 2016. The concept and algorithm is the same except that it's in a more advanced state then back then.

If something is stored electronically, you must know that it's easy to hack with the correct algorithm. Anyone can be hacker now days with the advancement of technology, things are becoming easy to use, accessible and largely most internet usage is not tracked as there is an overload of users on a server because of all the so called ‘smart-devices’. This is making things a bit difficult for cloud service providers and especially network service providers as they are dealing with new threats each and every day. Threats become more prevalent in everyday life, threat's to any technological device that uses wireless technology, this can include printers, a POS card system, mobile phones or basically anything that is based on a system that converts and transfers data and information. This is extremely unreliable to invasion of any kind, virus attacks, phishing, viruses of high intent against data and information.

As shown in Figure 1, cloud computing devices that can be used to access and store data via mobile and network service providers. The most relevant definition is the access of information through network and cloud service provider via the web.

Figure 2, explains the layout of how the cloud computing services to fulfill the customers requirements. This can have major and successful operations for a user, a cloud provider and a network service provider.

Cloud computing is the fastest growing software on the market at the moment, with vulnerabilities, being in its early stages of development, has caused some serious malfunctions of for some cloud providers, these can range from lack of network to an actual attack against the user (cloud provider). But for now the definition of cloud computing begins with storage of information from hardware to software built into a server by a cloud service provider\(^4\). The combination of Cloud Computing and IOT brings future innovations in the World Wide Web. The new thoughts coming from this integration is called Cloud IoT. It is a new creativity on Research and Development of Cloud\(^5\).

Figure 1. Cloud computing service system.

Figure 2. Layout of cloud computing operation.

Nowadays, cloud computing is accessed easily via mobile devices. These mobile devices have to be constantly connected to a network, which in turn provide
you the service of storing and receiving stored data and information. Security plays an utmost importance in today’s day and age, as humans need security to know that we are safe from harmful elements and know that we always protected. Security is defined as “the state of being free from danger or threat”. Transport Layer Security has been introduced, “Secure Sockets Layer (SSL)”, by in 1996. Cloud computing and its securities play a major role in almost every form of technological existence. We as humans are very easily persuaded by things, which can actually harm yourself, your family and another person. The best defence is to create that sense of safety and always 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 important to always be aware and on the lookout. Figure 3 illustrates the various Cloud Services provided to its users and how it operates.

Software as a service or SaaS:
The capability required to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are easy to get to from various client devices on either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

Platform as a service or PaaS:
The facility supply to the consumer is to organize onto the cloud infrastructure consumer acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not control the infrastructure such as network, servers and operating systems but has control over the deployed applications and possibly configuration settings for the application-hosting environment. This indirectly provides the necessary service to all, the user and its cloud service provider.

Infrastructure as a service or IaaS:
Infrastructure plays a massive role in everyday life, which include a house, a road which we use for transportation but infrastructure in cloud computing means exactly the same thing, except that it does not allow complete access from cloud service provider.

It provides various resources for the user of corporate companies like servers, networking, storage and data. Some cloud service providers charge for the amount of data and information stored on their servers as a pay-per-use basis/ for the amount of space used.

These are the three main cloud services and these have a major influence in how cloud computing works. Upon discovery, these services are very vulnerable against attacks such as Trojan attacks and more famously phishing. Hackers are developing algorithms to infiltrate users cloud storage via these various and stealing personal information, such as bank account details etc.

2.1 Several Areas of Concern Regarding Security Vulnerabilities of Cloud Computing

There are multiply ways an issue such as security can be major regarding cloud computing, the simple idea being the lack of network coverage, physical error, transparency, issues regarding the providers(network and service) etc. As shown in Figure 4 explains where and what cloud computing is used for various computing agencies.

Cloud computing is becoming more advanced but disturbances such as viruses, lack of network coverage and unreliability by network service providers are causing major troubles for a cloud service provider and its users. Things such as:

- Lack of network coverage is a major issue regarding cloud computing as clouds require an active internet connection. If not this can stop uploading of important information and can in other words lock a cloud if the provider has sensed an
issue. This will cause major disruptions and security for a user will be open to attacks as errors won't be or go un-noticed.

- Physical error could refer to loss of physical control of computer user and his cloud storage. Once the loss of data occurs, a range of problems arises such as privacy issues, risks, legal problems such as if a hacker gets hold of private info, this can ultimately affect a user. This will have major consequences on almost every concept of cloud computing.

![Figure 4. Uses of cloud computing.](image)

According to Vic Winkler explained that the main hope of cloud computing is network connectivity and bandwidth. Based on the demand, we utilize the cloud storage data. The lack of network coverage causes various problems in a cloud, for the user and for a service provider\textsuperscript{10,11}.

Things can go out of proportion:
- **Cloud Provider Viability**: The new cloud providers do not have technological knowledge about the cloud and facing the complexity on their viability, commitment and authenticity in the ever growing field of technological development. As explained earlier, clouds are still developing, so there might be an error or a problem there which is why some service providers provide a 24/7 service center for users to contact in times of need. For example, Google has a 24/7 customer service center and Yahoo has standby on demand customer service operators.
- **Transparency**: Cloud providers don't explicitly mention their internal protocols and technological advancements, thus indirectly implementing a trust from its users as they must trust the provider's security claims, that it is safe and reliable. This is a major concern going un-noticed now days as people (users) are blindly following advertisement.
- **Loss of Physical Control**: This can range from almost breach in protocol from users to service providers not providing the needs of user, unable to find the required data and its applications\textsuperscript{12}.

It deals with the following parameters like:
- **Data Privacy**: In public cloud data does not stay on the same system which arise the multiple legal concerns. These legal concerns can have major implications against users and the service providers as a whole.
- **Data Control**: A service providers IT division has less control scope within the IAAS layer implementation and still lower in PAAS layer. Users must have efficient that the provider assures the optimal control structures and solutions to all problems arising while keeping in control what data that is being used.
- **New Risks and Vulnerabilities**: The main complexity is the function of a network and cloud computing service provider's implementation to its users. Thus leads problems on all software, hardware and networking equipment, which are focusing the detection of vulnerabilities like security risks imposed on cloud computing from various elements. But by simply applying layered security software's, improving the algorithm of cloud computing elements and its operations, we can safeguard from common attacks from increasing security issues.
- **Legal and Regulatory Compliance**: Usage of public cloud data subject to regulatory compliance from governments or organizations that are restricting you from using some advances and techniques while saving onto a server. Cloud providers is to address the needs of regulated markets in developed nations, while in undeveloped nations; it is still in a process of restriction due to the lack of required skills and infrastructure. The optimal practices, development and better understanding for cloud computing provides a better, greater scope for development.
and this concern should be able to fade away. As shown in Figure 5 explaining the cloud computing concerns in security risks and privacy.

![Cloud Computing Concerns](image)

**Figure 5.** Security risks and privacy.

### 3. Methodology

There are ways to initiate service providers to create safer clouds by simply securing cloud computing servers. This can be done in many ways and is currently the safest way to make sure your data and information is safe because these use an extremely advanced algorithm, which is biometrically safe. This methodology will create the most important security safety for any user and that is awareness. By simply inputting a security scanner before saving onto a cloud activation and log-in for its users, can create more viable software.

Therefore, implementing various security checks upon registering and giving the user options for its security to provide easy to use functionality is of great importance. This password may be advanced such as bio-metric scanners such as finger-print scanners already used on most mobile devices and is found to be a safe way to store data on a device like a hard-drive.

There are four levels in cloud security and it is explained in the Table 1.

Another method is to counter the ever growing demand for network access in both urban and rural areas, with rural areas being the most affected. Some people want to access their information from a cloud almost everywhere the need be and network access can cause major disruptions in a clouds functioning, for example, if the network cuts off, the document could not load onto the cloud causing distortions in data and lack of it thereof stored on the cloud. To counter these problems, such as lack of network, this disrupts a server linking onto a cloud computing server because of lack of network coverage etc. This can cause a cloud to lose all of its information and sadly its stored data as a cloud server might depict a system crashing, (which can cause all stored data to delete, if the cloud user has not saved its data onto the cloud server) the best way is if the service providers of a cloud and also its users work with each other to achieve ultimate security. The best thing for a user is to report issues regarding cloud to their service providers (cloud and also their internet providers). The solution for network availability is simply the creation and viability of web to cloud service providers. Web and service providers desired to examine the control issues, techniques to prevent loss of signal, such as improve their coverage in areas that are hard to reach and provide more concise network signal coverage in urban areas. This is done by getting the attention of a user by giving the wrong impression and then making the user aware of his mistakes. This will require an advance algorithm from computer programmers but it can be done.

<table>
<thead>
<tr>
<th>Security</th>
<th>Level and whose responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>This includes the browser, cloud log-in and server security authentication. All done by the user to service providers.</td>
<td>Level 1 is user layer.</td>
</tr>
<tr>
<td>This is the data transmission area provider by the service providers to the user.</td>
<td>Level 2 is the network providers such as cloud and network.</td>
</tr>
<tr>
<td>This includes virtual computer authentication, which is a computer to server security identification.</td>
<td>Level 3 is both user and network providers.</td>
</tr>
</tbody>
</table>
This includes network, data, and server storage authentication and its security.

Level 4 is the important security check and it’s both the users and networks final responsibility upon accessing each other’s data and information.

These advanced algorithms need to be constantly in the run and updated by skilled programmers alike, this will keep intrusions on a cloud service hard to come by. These can go a long way in providing the safety a user wants and also the smooth process for service providers alike for a return in their investments. In the Figure 6 illustrates the main uses of cloud computing areas.

Figure 6. Main applied areas of cloud computing.

3.1 Steps to Improve Cloud Security

- Make sure a user know whose accessing what and watching your every move:
  Every organization has a trusted IT administrator who can make any changes regarding their computers system or their clouds.

- Users must limit their data access based on what a user is going to use it for:
  A user must always be aware and continuously changing the limit of accessibility of their data, depending on where the user is and what device they are using. For example: When a person uses a mobile device, he/she has to go through additional sign-on steps and has more limited access to the data.

- Risk-based methodology is used to secure assets such as valuable information stored on a cloud and that’s used in the cloud:
  Thus encrypt and provide extra protection for valuable datas.

- The use of extending security software to the device that is being used:
  Make guarantee that corporate data is secluded from personal data on the mobile devices, such as tablets, smart-phones. Scan mobile applications from time to time to check for security risk and this can reduce to prevent loss of physical control, such as data lose and privacy.

- Add artificial intelligence to network protection
  The intelligence roll can be used in multiple ways, with its prime development being protection of its network’s service being provided to cloud operators. This will make a user feel more secure in his attempts to use cloud computing properly.

As shown in Figure 7 illustrates the graph from Google.com showing that the increasing trends in cloud computing.

Figure 7. Trends in cloud computing.

4. Results and Discussion

The future development of cloud computing is to provide a 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 in the growing field of the cloud computing industry as a whole. Thus this can improve its security issues and develop a more concise cloud computing product.

The generic design principle of a cloud environment is to control relevant security risks and threats. It needs a systemic point of view, from which protection of data on trust, justifying security to a trusted third party\textsuperscript{20}. Cloud security concerns that impede the high rate adoption of the cloud computing. The cloud users are well known about the existing security threats in the cloud. This leads minimal cost estimation in their security risk development. Earlier the cloud computing offers conventional technologies and unique security issues. Currently virtualization allows various users (possibly from different origins) to utilize same physical resource\textsuperscript{21}.

The discussion evolved on whether or not cloud providers and internet service providers will be willing to invest their money into something that can take time to achieve. This result is also achieved by cloud and search engine companies such as Google, who have taken the necessary steps to improve their cloud computing servers and have been a success. They have implemented steps to recover hacked cloud accounts and have taken precautions against attacks in their cloud computing server. It requires co-operation of organizations, government and users. This can be achieved but it will take some time. Thus improve high reliability, efficiency and create a sense of security in cloud computing\textsuperscript{22,23}. Cloud computing is a recent innovative field, which came into existence after long research in networking and various types of computing. It utilize a SOA, that minimized the information technology operating and maintenance cost for the clients, gives greater flexibility, reduces capital costs, issues required services are along with many other characteristics\textsuperscript{24}.

5. Conclusion and Future Work

The projected methodology has a good ending and can build trust with many service providers. Trust is more imperative and make the triumph of cloud computing. A cloud offers a path to efficiency, reliability, security and offers very useful, easy to use control. Cloud computing companies are taking initiatives in improving security issues, network issues and providing a stable background to smooth functionality. Organizations, industries and users should select their cloud providers with intense scrutiny and ensure they pick the best. This is to concerns that the security risk concentrates on physical, software and cloud security. As discussed throughout the area of cloud computing, users have to be more aware of that they are simply doing online and create a sense of safety for themselves and this can be created using the cloud provider’s innovations. Ideas, innovations and creativity can go a long way to create an idea of ultimate safety for the providers and for the users as a whole. Currently cloud computing is adopted by many corporate companies and challenging the various issues like load balancing, network security, and cloud green computing which have not been fully addressed. These are now being addressed by the concerned parties and we look forward for a safer, better, more advanced cloud computing in the future. A more convenient way in cloud computing is needed and this can take a while for it to be perfect in every-way. Certain cloud providers are taking huge steps in dealing with cloud computing security issues and are planning major developments for it to be extremely safe against attacks and error free. This can be achieved and when considering a move to use cloud computing, users must have a complete knowledge of the potential security benefits, risks and realistic expectation with their cloud provider, for it to be extremely functional and safe. There must considerational as its still in its development stage. Certain infrastructures such as IaaS, PaaS and SaaS can each play major role in securing the future of cloud computing. This bring along additional security requirements and responsibilities. This paper highlights the role, users, service providers such as network and cloud computing play in protecting and safe guarding cloud development. This can prove to be the future and the future can be made sure of safety. However, this is a learning step to success.

6. References