Analyzing The Protection Of Cloud Security Against Cloud Security Risks With Secure Coding Mechanisms

Anees Alam[1*], Dr Vaishali Singh[2]

[1*] Phd Research Scholar, Computer Science MUIT Lucknow
[2] Assistant Professor, Department of Computer Science, MUIT Lucknow

Abstract

Cloud computing is a technology that supports data and applications by using a central server and the internet. The user can use the Internet to access the application and data from any computer. By combining processing, bandwidth, and storage memory, this technology enables far more efficient computing. One method that supports all IT operations is cloud computing. Rather than relying on internal performance and infrastructure, it utilizes on-demand IT services to remove the technological barriers that organizations must overcome in order to design information. Because organizations save their most sensitive data on the cloud, data reliability is the main problem when discussing cloud computing. Cloud computing has an issue related to security, which is why cloud user are always not sure about the security of data that they maintain on the cloud. The safety issues concerned with cloud computing is high.

Finally, by incorporating strong secure coding techniques, this paper hopes to help developers, cloud service providers, and security professionals improve the security posture of cloud infrastructures and promote a more secure and resilient cloud environment.

Keywords: bandwidth; data security; Central Server;Cloud Users; IT Operations

Introduction

The field of cloud computing is expanding within the computer industry. It is a cost-effective method of maximizing computer capacity and use without having to invest heavily in new infrastructure. Services provided by cloud computing offer several benefits, including element property, profitability, dependability, adaptability, and liability. The cloud's resources can be extended in any direction based on the client's requirements to improve the assignment's execution.

The main component behind cloud computing is the data center. The data center refers to an on-premise hardware facility that is use of much purpose.Cloud computing is a type of computing that provides an off-premise computing facility like storing data on virtual resources using the Internet.

Cloud computing offers services instead of product, whereby shared software, information and resources are supplied to computer and other tools efficiently over a network. Cloud users should not need to identify the site and other particular such as infrastructure but cloud computing offer software, application, computation, storage resources and data access and data a   administration facility.

End user access the cloud based application via diverse interfaces such as light-weight desktop, a web browser or different mobile application, where application such as data and business software are saved on server at an isolated site. The suppliers of cloud computing attempt to provide improved functioning and service than thatprovided when software programs were deployed locally on the end-user or on detached computers.

Cloud computing performs task at a faster rate to meet the demands of user it permits the data center to allow enterprises to acquire applications and works on data quickly and needs only simple administration and less upholding. Many unpredictable and uncertain company orders of IT resources, such as networking and servers, are effortlessly meet with the cloud computing technology.

The initial structure of cloud computing is shown below. As given in the figure facilities and services are offered by cloud providers in a cloud computing environment and different user from various locations and devices can request for specific service that are offered.

There are three types of services in cloud computing which are discussed further. Software as a Service (SaaS) allows several customers to access a single customer-prepared service on-demand from a single cloud.

Therefore, it is not necessary to buy a new server or any other platform.Instead of setting up their own physical infrastructure, the users ordinarily prefer a mediator provider for the service of the internet in cloud computing. The users have to pay only for the services they had used **[1]**.In cloud computing users have to only pay for the services they consumed. Maintenance cost is low as user do not need to purchase the infrastructure**[2].**

There is a real-world example which is that if a user wishes to buy Windows OS rather than Ubuntu, they should contact the cloud provider and pay the appropriate amount. Some websites, such as Microsoft Azure,

Salesforce.com, and Google Docs, operate on the Software as a Service (SaaS) model. Platform as a Service (PaaS), wherein the platform for developing and sustaining applications is made available. Examples include Force.com, Microsoft Azure services, Google App Engine, and so on.

According to the some sources, Infrastructure as a Service (IaaS) offers data centers, network capacity, storage for rent, and other services. Hardware as a Service is another name for it (HaaS).

Basic Structure of Cloud Computing
Related work
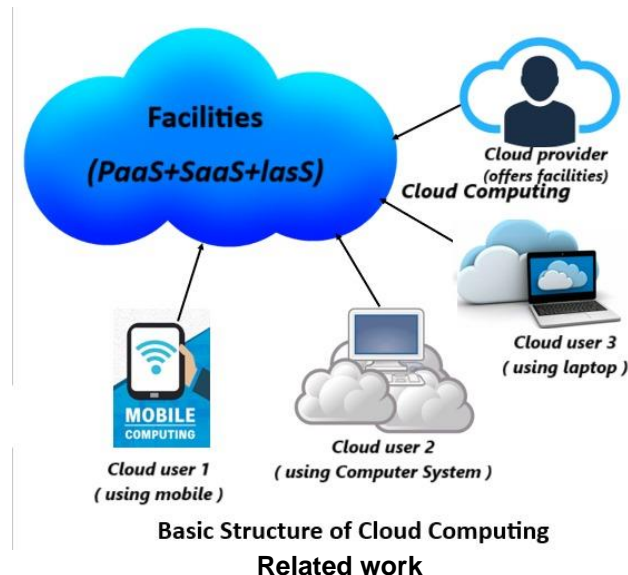
1.Cloud Security Risks

Cloud security has emerged as a critical area of concern as cloud computing services proliferate across various sectors. Several studies have identified and categorized cloud security risks, including data breaches, account hijacking, insecure interfaces, and data loss. For instance, Subashini and Kavitha (2011)**[3]**provided a comprehensive survey on the security issues in the cloud, emphasizing the need for robust security mechanisms to protect data integrity and confidentiality. Similarly, Hashizume et al. (2013) **[4]**discussed common vulnerabilities in cloud environments, highlighting the importance of identifying and mitigating these risks proactively. Besides legal security requirements, it is necessary to address some basic security requirements like authentication, integrity, transparency, confidentiality, availability and audits as stated in Rebollo.**[5]**

2.Secure Coding Practices

Secure coding practices are essential to fortify applications against security vulnerabilities. McGraw (2006) **[6]**introduced the concept of software security through secure coding, illustrating how incorporating security into the software development lifecycle can mitigate risks. Studies by Howard and LeBlanc (2003)**[7]**demonstrated practical applications of secure coding principles to prevent common security flaws such as buffer overflows and SQL injection attacks. The importance of integrating security checks into the coding process to detect and resolve potential vulnerabilities early has been widely acknowledged in the literature.

3.Mechanisms to Enhance Cloud Security

Various mechanisms have been proposed to enhance cloud security. Encryption, for instance, has been extensively studied as a primary method for protecting data at rest and in transit. A survey by Khan et al. (2013)**[8]**discussed encryption techniques and their effectiveness in ensuring data security in cloud environments. Moreover, the implementation of robust authentication mechanisms has been identified as crucial for preventing unauthorized access to cloud resources. Fernandes et al. (2014)**[9]**explored authentication methods in cloud computing, emphasizing multi-factor authentication as a key strategy.

4.Role of Secure Coding in Cloud Security

The intersection of secure coding and cloud security is a relatively newer area of exploration. Gupta et al. (2016)**[10]**examined how secure coding practices could be tailored specifically for cloud applications, identifying unique challenges such as multi-tenancy and shared resources. Their findings suggest that incorporating secure coding mechanisms can significantly reduce the risk of vulnerabilities that exploit cloud-

specific characteristics. Moreover, Sharma and Chen (2017**0[11]**discussed how secure coding standards, such as OWASP and CERT guidelines, can be applied to cloud development processes to enhance security.

Essential of Cloud Computing

As cloud computing is a recent technology and modern computing paradigms, different people have different views about it. Cloud computing actually meet the overall software and hardware demand of an organization, user, or company. Cloud computing is a novel approach and an important innovation in how we operate application and saved information. On the cloud, everything is hosted effortlessly. As compared to personal desktop it's easier. Globally you can access any record or any application from any source. Some of the benefits of cloud computing are given here

1. For fast accessing, It improves parallelism and allocation of resources
2. And additional company host a set of application, get software renewals(with no charge), and so on.

One may acquire software services networked storage space, computer resources and various other services at a single place.

3. It improves monetary burden such as operational expense renewing charge, and capital expenses

There are two types of cloud environment:

1. The end user who has no idea about cloud complexity.
2. The cloud service provider who has the liability of controlling the complete cloud environment and other services to the consumer. One of the jobs of the suppliers is safety and it ensures the consumers the degree to which their data is protected. The cloud service supplier is also accountable of IT resources, uploading and other services offered to the user. Various services and resources are provide to user by the cloud provider, as suggested and a managed by the cloud administrator in the cloud environment as shown in figure below.
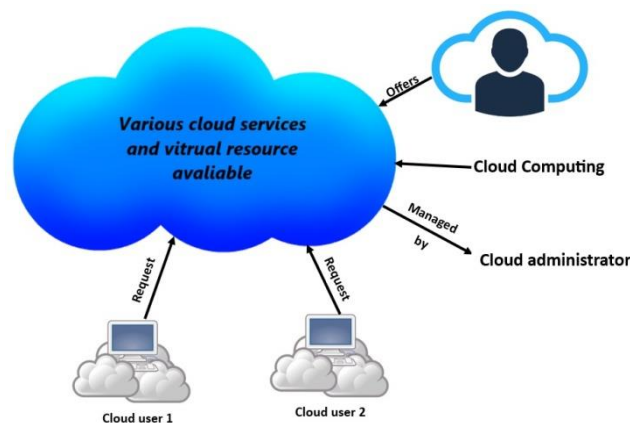
Cloud resource management

Cloud computing gives users the option of accessing information from any place at any point of time. To access the conventional computer system, you should be in a similar physical position as your data storage tool. The cloud eradicated the barrier. Suppliers of clouds offer you the mandatory software and hardware for operating your company or home applications. You require an Internet connection to access the cloud. The benefit is that you can access that record from anywhere, by any tool that can access the Internet. Workers at distinct sites can access similar data on the cloud and any tool may be used (eg. Laptop, desktop, mobile phone, or tablet) Cloud computing involves a cloud consumer, cloud provider, cloud broker, and cloud

Terminology used in Cloud Computing

Cloud consumer	An individual person or organization that sustain a business relationship with cloud providers and avails the services offered by provider
Cloud provider	An Individual person or organization who offers a service and is liable for the services of cloud computing of the parties that demand it
Cloud auditor	A party that conducts evaluation of cloud services such as performance operation on various system and security
Cloud aggregator	The management part between cloud service providers and cloud consumer, like provides the services to consumer
Cloud transporter	The mediatory responsible for connectivity and transport of cloud services from service to cloud consumers

Need Of Cloud Computing

The desires of every corporation are to provide workers a comfortable platform for working. In a corporation, there are top-level professionals who are always in the pursuit of more elasticity, heavier workload at lower fees, and the use of information as a competitive benefit to recognize the most appropriate information and data for decision-making. IT corporations need to react to these changes by converting IT into a domain with better business agility.

Cloud computing offers services to users for storing software and files distantly, instead of on a server or a hard drive at their workplace. Every corporation must possess its own personal cloud that may be adapted according to the users' demands. Examples include video sites such as Facebook and YouTube, web-based email such as Hotmail and Gmail, conversation support tools like Skype, and many others. Certain cloud computing applications comprise Software as a Service (SaaS), file storage, and file back-up, file synchronization, and consumer relationship management. There are many benefits of using cloud computing for worldwide corporations. One of the key reasons is the elasticity provided by it.

Through the Internet, employees may access information from home, on the way, from a customer's office, or from a smartphone such as an iPhone or a BlackBerry. Employees may also jointly work on documents and files, even when they are not physically all together. Everyone can work mutually even ifthey are in remote areas.

they are physically far from each other. Proofreading of documents and seeing them can be done at the same time.

Cloud computing is quick and hassle-free to operate. Since downloading and deploying of software needs time, clouds maintain everything up to date. Cloud computing is cheaper as well. There is no requirement of purchasing and deploying costly software as it is already deployed online and youoperate it from there. Cloud computing provides agility and it may be easily and swiftly scaled up and down as per the requirement.

One of the chief benefits of using cloud computing for various corporations is that it provides nearly infinite storage, in contrast to a server, and takes into consideration the limits of a hard drive as it is online. We need not to recompense for huge disk space and devices. There are many challenges associated with a conventional infrastructure:

Software licensing and support Licensing of application and data centers is needed. For assigned data centers ,in cloud computing, single license is required for application.

Scalability Conventional infrastructure cannot extend easily at a particular instance of time, and scalability requires variation with time. In order to face the challenges, it has to be regularly improved time to time.

Accountability Not even a single instance in history, conventional infrastructure in application has important liability and powers.

ModifiabilityThe application continuously requires and sustains extra charge even when alteration is needed.

Physical securityphysical security is even now a complicated issue related to cloud computing and its' hard to sustain security.

Cost-effective management The redundant data is required regularly to make application significantly accessible which is very cost efficient for an organization. Even after decades of augmenting data center and IT development most of the companies are left undealt with complex and overgrown computing plat form.

We have discussed several benefits of cloud computing in the following section in details which has brought about a revolution in the era of computing:

Reduced Costs

Cloud technique is rewarded inclemently, thus it can be use in helping in the reduction of expenditure to an organization., IT expenses can be minimized With the help of cloud computingFor example, , you need not deploy and set up any resource at your own risk or cost. if you are offered a business application over the Internet.

Because of Expenses of maintenance and up gradation are handled by the cloud provider Cloud computing services can minimize the updating requirement of software and hardware. The cloud provider handles complexity of technical proficiency As it is permitting users to concentrate on their main business. IT cloud computing follows a pay-as-you-go approach because here only a low preliminary investment is needed. The main cause of companies to use cloud computing is to save funds. The technology used behind the cloud

eliminates the servers' cost, maintenance fees, data center space, software licenses, etc. Hence, minimized and substituted asset expenses are scalable and convenient operating costs.

Another aspect that should be taken into account while we select the cloud is that customer organizational support and maintenance expenses are minimized drastically as these costs are shifted to the cloud supplier, comprising 24/7 support. IT recruits is minimized as well because the requirements is extremely trained and costly. The resources are used more effectively, resulting in considerable support and saving of energy expenses in cloud computing.

It has been discovered, in practicethat companies spend almost double on server energy expenses than on hardware. By cloud computing, an option has been provided or these costs. With the help of cloud computing, corporations need not purchase and deploy costly platforms and software in order to host the software. Instead of many cloud computing applications being provided cost-free, end users are just needed to subscribe to services desired by them, rather than purchasing necessary software. You may scale up or down according to your desire and requirements.

SCALABILITY

With the help of cloud technology, more information can be saved, when compared to the personal computer systems used by the companies. Some of the major advantages of scalability are as follows:

1. As the business pays only for the services it avails, it becomes one of the biggest advantages of cloud computing. Businesses should invest in advanced storage tools and servers which normally occur at fixed prices in a conventional infrastructure and technology. Cloud computing is exclusively scalable and flexible, functioning on the basis of permitting businesses to pay as per work and the resources used by them.

2. Since cloud computing is completely based on virtualized technology, RAM space, storage, etc., are simple and swift to append and use. The requirements of a business can be attained or accomplished in hours rather than days.

3. In a cloud environment, scalability is a major benefit. Further resources are includedwith the expansion of the business, to support the progress of the business. In association with SaaS, businesses have to pay according to their demand, that's pay more for more demand and less for less demand.

4. As the business requirements rapidly go up and down so instead of buying and making costly advances by yourself, your cloud service supplier may deal with it for you.

5. As this service of cloud computing frees up your time, you may focus more on the functioning of your business.
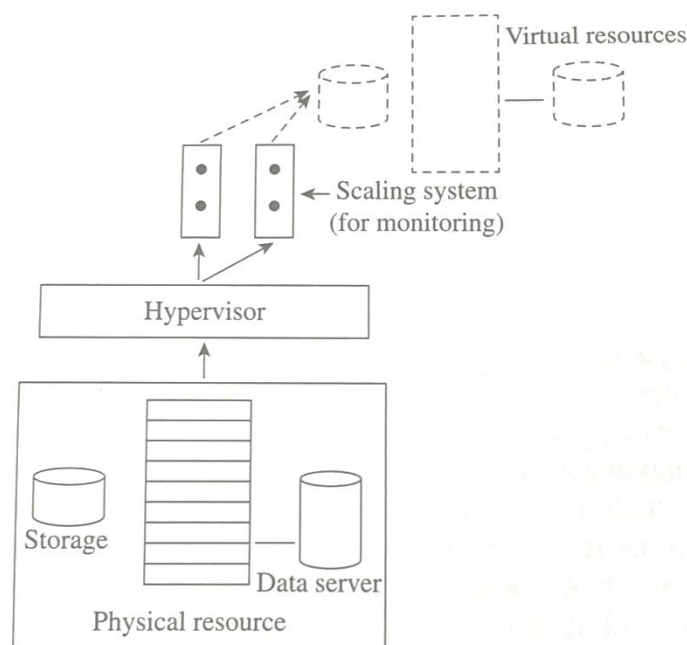
1.3.3 Remote Access

To synchronize data access between international offices through cloud computing, it becomes very easy
Once data is virtually stored, it can be shared fluently between offices that are far from each other through isolated access Any tool can be used, any time and at any place that's an advantages of isolated access are that

Anytime, access to Viewpoint V6 Software is offered by Viewpoint Cloud Computing and it is the top incorporated comprehension software solution of the industry that can be accessible from any place with an Internet connection.

Regardless of place, users would have access to their software, attributing the newest information and data on any venture. Users can do the following:

1. Access project reports and data, alter orders, etc.

2. Sense the 'always on' benefit of being capable of giving up one zone and carry on even on your smart cell phone.

3. Expand your trade and support your cell phone sales strength as everybody has 24 x 7 access to the cloud any time, from any mobile tool or desktop.

The advantages of cloud computing and web-based business cooperation applications all emphasize on the advantages of isolated access. Cooperating on shared records expands the speed upon which people may complete complex jobs collectively. Accessing private files from any isolated desktop connection signifies that a person is certainly not coupled to a machine or site in order to use software and files that are vital to them, whether for personal or business use. Web and cloud computing are as good as the extent to which they facilitate people to share and access; isolated access is the chief advantage of these technologies.

Isolated access functions in three fundamental methods. The first is the streaming of data from one machine to another; this occurs when a person online listens to a radio station or watches a movie.

The second one is when web applications exhibit an interface which permits the web user to interact with an application such as an online store or a search engine. The third one is when files are made comprehensible on an isolated desktop computer through desktop sharing and isolated control software,. For the third use, users download isolated PC access software, a petite yet precious piece of software for small ventures and also for large- and middle-sized businesses.

Disaster Relief

Natural calamities such as earthquakes, floods, internal troubles, and wars might result not only in the loss of data of e-governance applications but also in unavailability of services. In a different geographical locality, multiple set-ups along with total backup and retrieval explanations should survive. Disaster recovery control measures should be put in place and exercised from time to time. Data and applications should be surplus and must be accessible at short notice to switch from one data center to another. Cloud virtualization techniques permit restoration and backup. As compared to a conventional data center, it provides flawless migration of applications.

HISTORY OF CLOUD COMPUTING

The National Institute of Standards and Technology's (NIST) defines cloud computing [12] as, "Atemplate for providing the suitable and when needed access to the internet, to a collective pool of programmable grids, storage,servers, software, and amenities that can be rapidly emancipated, with little communication and supervision from the provider"

Cloud computing is an Internet-based service that has evolved after going through several phases, for example, grid and utility computing, SaaS, etc.

In 1999, Salesforce.com came into the market. This was a pioneer of cloud computing. After that, Amazon Web Services was launched in 2002, which provided customized cloud-based services including storage, computation, etc., to the cloud

users. Another big invention in cloud computing was in 2009, as Web 2.0 and Google services, through Google Apps .

Benefits of cloud computing

Cloud computing technology offers various benefits to both cloud service consumers and cloud service providers. The main advantage of cloud computing systems and technologies is increased economical return due to reduced maintenance costs related to infrastructure and IT software. Capital costs are costs associated with assets that need to be paid in advance to start the business. Before the advent of cloud computing, software and IT infrastructure generated capital cost, since they were paid upfront to afford computing infrastructure and software for enabling the business activities of an organization. The business revenue is utilized to pay off over time for these costs. In case of hardware, it is always associated with depreciable values. To make profit, the organizations have to also compensate this depreciation created by time, thus reducing the net gain obtained from the revenue. In this way, cloud computing technology transforms IT infrastructure and software into utilities. Cloud computing offers the following benefits:

1. Pay as per use

2. reduced investment and proportional costs

3. accessibility from anywhere

4. increased scalability

5. increased availability and reliability

6. Dynamic provisioning

7. Increased data safety

8. Improved performance.

9. Lower software cost.

10. Increased computing power.

11.Unlimited storage capacity

12.Latest version available.

LIMITATIONS OF CLOUD COMPUTING

Cloud computing is broadly acknowledged as a revolutionary IT concept and along with customized assistance may suit the requirements of various consumers, scaling from big ventures and small beginners to end users. Many cloud-based applications like Gmail have become very successful; however, in the information technology departments of organizations and corporations, the decision makers continue to refuse to use the cloud.V. S. K. Maddineni and S. Ragi[13] have identified forty-three security issues in cloud computing, such as denial-of-service attacks, data leaks, and data availability. Furthermore, the incidents that happened in 2009—when Amazon's basic storage service stopped operating between February and July—amplify these users' concerns. Similar to this, in May 2009, hackers targeted Google Gmail, causing it to become silent for four hours. In a similar incident, Microsoft Azure had a 22-hour suspension and suffered a 45% loss of client data [14]. A cloud storage company called Drop Box suffered after passwords were stolen from their database, allowing everyone to access their data [15]. Currently, companies mainly just contract applications which comprise less confidential data. The ones which become ready to move to the cloud still insist on third-party risk appraisal or enquire with cloud suppliers on the following:

1. By whom the applications and data will be accessed and how will that be examined?

2.What security methods are used for storage and transfer of data?

3.How data and applications from diverse consumers are reserved separately?

4. In terms of geographical sites where will the data be stored? Will the selection of the site influence us?

5. Is it possibe these details and channels be specified in a service-level contract?

Each of these consumer worries are the chief obstacles to the implementation and development of cloud computing. Some of the restrictions of cloud computing are discussed next.

1.8.1 Availability of Services

By the Internet only consumer administration interfaces of public clouds are possible .

As services are a primary concern of consumers, they sometimes need to discard all the data from the cloud environment provided to them, while sometimes they may want to recover all the data. There is an augmented risk of disaster in this when compared to conventional services, as there are more ways to access the application or information over cloud computing.

2 Data Lock-in

SaaS permits services to be interoperable on every cloud. However, shifting of data and applications from one platform to another is a challenge to the cloud provider for a big organization handling high volumes of data. Google is the single cloud supplier to attain a more typical environment and they also have a scheme, known as Data Liberation Front, to support user shifting applications and data in and out of their platformof their platform.

Data Segregation

It is not simple to isolate cloud users from each other. A straight effect of the multitenant control mode, where virtual machines of distinct consumers are co-located on a single server or data on single hard disks, is the main concern related to privacy.

This is the set of risks which comprises matters regarding the break-down of mechanisms to separate memory or storage with distinct users.

Amazon EC2 service consideredthis as a real threat and rectified this attack by successfully overcoming the following:

1. Actually this has to be finding out where a particular virtual machine command is located in the cloud infrastructure

2. To In a similar physical machine whether two instances are resident or not.
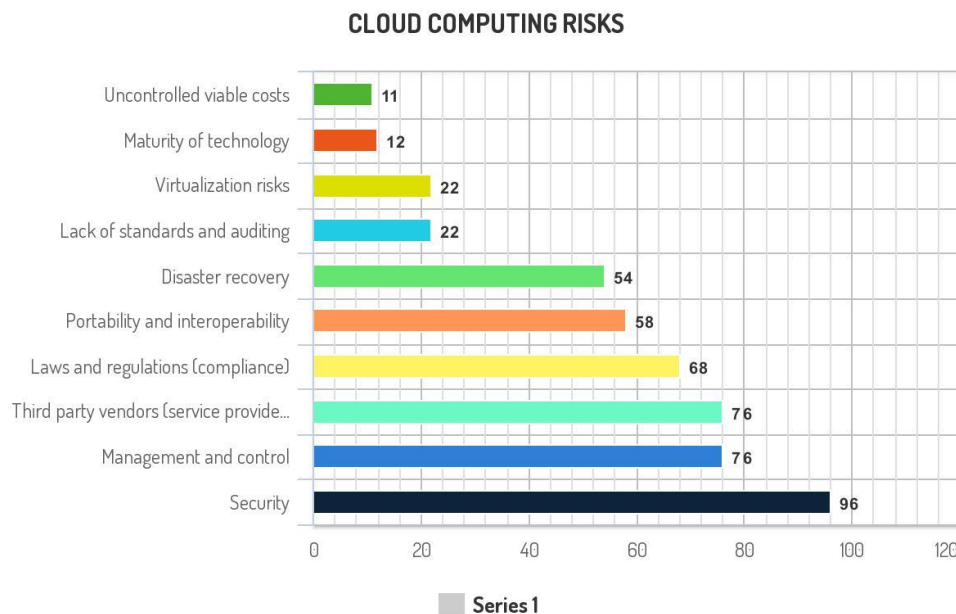
3. The secrecy of the data should be guaranteed, whether or not it is in transit. It should be required to offer a closed box implementation environment where the secrecy and reliability of the data must be confirmed by its possessor.
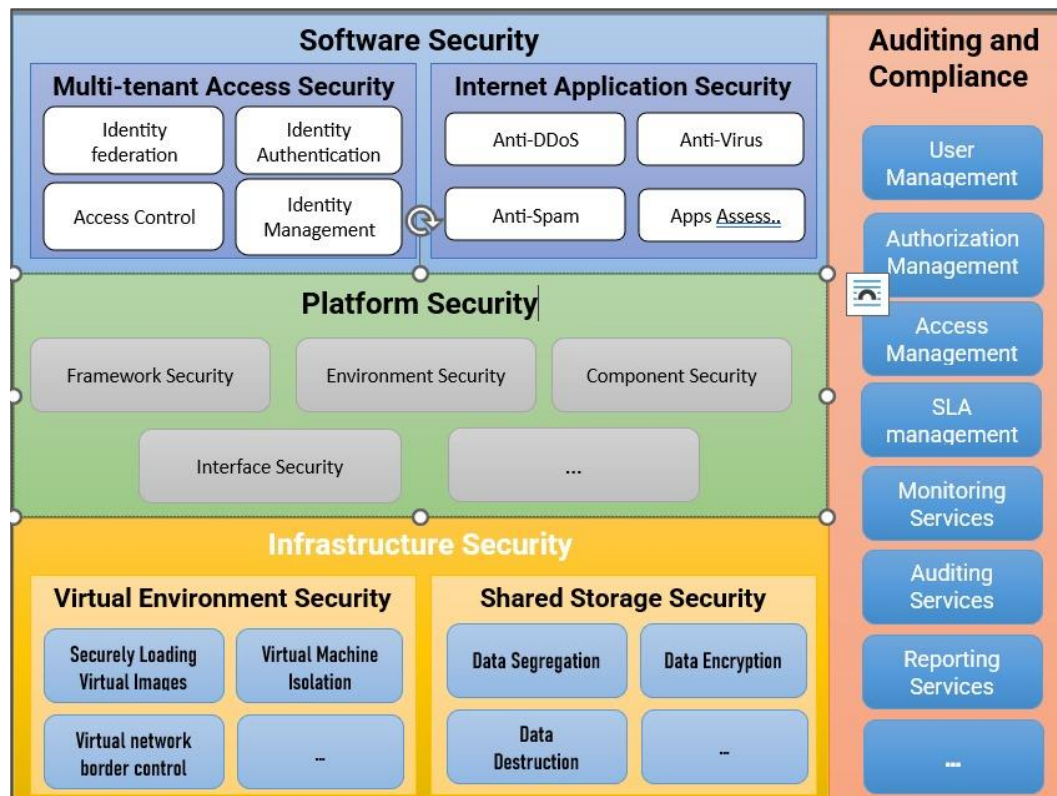
4. In a majority of circumstances, data should be encrypted at a certain time when it is within the cloud. Several procedures are unfeasible to perform with encoded data, and moreover performing computation with the encoded data must utilize more computing resources.

5. Before uploading to the cloud data should be encrypt. When specific data is needed, the token creator is used by the user to produce a token as well as decryption key. The token is transmitted to the cloud, the chosen encoded file(s) are downloaded, and after that these files are confirmed locally and decrypted using the key. Sharing is facilitated by transmitting the decryption key and token to the other user with whom you wish to cooperate.

Cloud computing Risk Graph

CLOUD COMPUTING RISKS

Category	Value
Uncontrolled viable costs	11
Maturity of technology	12
Virtualization risks	22
Lack of standards and auditing	22
Disaster recovery	54
Portability and interoperability	58
Laws and regulations (compliance)	68
Third party vendors (service provide...	76
Management and control	76
Security	96

Series 1

Cloud computing Security Architecture

Fundamental Exploration Multitenancy, the act of facilitating various inhabitants (clients or associations) on a common cloud framework, brings various benefits, like expense productivity and asset enhancement. Notwithstanding, it likewise presents a bunch of difficulties and expected issues. Here is an outline of the multitenancy issue in distributed computing:

Security Concerns:
Information Detachment: Guaranteeing the total confinement of information between inhabitants is testing. Lacking safety efforts could prompt information spillage or unapproved admittance to delicate data.

Shared Assets:
The sharing of assets, including registering power and organization transmission capacity, builds the gamble of safety breaks on the off chance that appropriate disengagement components are not set up.

Execution Issues:
Boisterous Neighbors:
The presence of "uproarious neighbors," where one occupant consumes an over the top measure of assets, can influence the presentation of different inhabitants having a similar foundation.

Asset Conflict:
High asset interest from one occupant might prompt asset dispute, bringing about corrupted execution for different inhabitants. Consistence and Legitimate Difficulties: Information Residency and Consistence: Various occupants might have explicit legitimate and consistence necessities, making it trying to guarantee that information is put away and handled as per material guidelines.

Auditability:
Data provenance [16] explains the origins of a piece of data and how it got into a database. Accountability, authenticity, and identification attacks benefit from data provenance and auditing. Following a summary of the the most advanced in cloud forensics storage systems, Ricci et al. [17] examined the problems and difficulties of a decentralized cloud database for digital forensics based on blockchain technology, using STORJ as an example.
Satisfying examining and consistency guidelines becomes mind boggling when numerous occupants with shifting administrative necessities share a similar foundation. Customization and Confinement:

Customization Imperatives: Suppliers frequently limit the degree of customization occupants can perform to keep up with the consistency and security of the common framework. Disengagement Intricacy: Accomplishing both asset dividing and confinement between occupants is a fragile equilibrium. Overemphasis on seclusion might prompt underutilization of assets, while lacking separation can think twice about. Reliance on Specialist organization: Seller Lock-in: Multitenant arrangements frequently attach occupants to explicit cloud specialist co-ops, making movement and change testing. Specialist co-op Personal time: Inhabitants are subject to the dependability of the specialist organization, and any personal time or administration disturbances can influence different associations all the while. Adaptability Difficulties: Scaling Hardships: As the quantity of inhabitants increments, scaling the framework to oblige development turns out to be more intricate. Asset designation and scaling should be overseen productively to guarantee ideal execution. The executives and Checking: Occupant Separation The executives: Nonstop checking and the board are expected to guarantee that inhabitants stay segregated and that asset usage is fair. Investigating Intricacy: Recognizing and settling issues, particularly in shared conditions, can be trying because of the interconnected idea of assets. Monetary Contemplations: Cost Designation: Deciding fair and straightforward expense assignment models among inhabitants can be multifaceted, especially when assets are shared progressively founded on request. Tending to these difficulties requires a blend of strong safety efforts, powerful asset the board procedures, and clear correspondence between cloud specialist co-ops and occupants. As distributed computing keeps on developing, progressing examination and advancements are fundamental to relieve the multi-occupancy issues and improve the general effectiveness and security of shared cloud foundations.

Objective
Establish a safe link that lets authorized users view information kept on a cloud server.
Example (Simple Explanation): Let's say you have confidential information securely kept on a cloud server. To ensure that nobody can decipher it without the proper key, you lock it up with a secret code.
At this point, you generate a unique token or key that only specific individuals may use to access and view the data. Similar to a secret password is this key.
How long this key works is up to you. Limited access is ensured because the key will no longer function after this point.
The locked-down data is then combined with the unique key to create a unique connection. Similar to a hidden address to the locked data, this connection can only be accessed by those with the unique key.
You ensure that the data is transmitted securely by sharing this link with just the individuals who should view it.
In this manner, even if the link is discovered, the data will remain safe because only the unique key will enable access to the data, and the link will expire after a predetermined amount of time.
By restricting access within a predetermined time window and requiring the correct access token for authorized users, this method makes sure that the link to access cloud data stays secure.

Algorithm of Data encryption and Decryption
1. Define a class **EnctyptionDecryption**
2. Define function **blankcheck**(n : type String)
3. N←n.trim( )   // To remove the leading and trailing spaces
4. return n.length() > 0
5. End of function
6. Define function **Encrypted**(n : type String)
7. Check if (**blankcheck**(n)== false)
8. return "Blank String is not allowed"
9. else:
10. Code← ""
11. Let len=length(n)
12. Repeat
13. For i=0 to len do
14. Let p=extract character from i position and store
15. Let d←p
16. if p>='A' and p<='z' then
17. d=d+10
18. if d>90 then
19. d=d-26
20. Else if (p>='a' and p<='z') then

```
21. d=d+15
22. If(d>122) then
23. d=d-26
24. Else if(p>= '0' and p<= '9' ) then
25. D=d+5
26. if(d>57) then
27. d=d-10
28. Let ecode=encode+(char)d
29. End for
30. Return ecode    //Encrypted code will be return from function
31. End function
32. Define function Decrypted(n : type String)
33. Check if (blankcheck(n)== false)
34.  return "Blank String is not allowed"
35. else:
36. Code← ""
37. Let len=length(n)
38. Repeat
39. For i=0 to len do
40. Let p=extract character from i position and store
41. Let d←p
42. if p>='A'  and p<='Z' then
43. d=d-10
44. if d<65 then
45. d=d+26
46. Else if (p>='a' and p<='z') then
47. d=d-15
48. If(d<97) then
49. d=d+26
50. Else if(p>= '0' and p<= '9' ) then
51. d=d-5
52. if(d<48) then
53. d=d+10
54. Let ecode=encode+(char)d
55. End for
56. Return ecode    //Encrypted code will be return from function
57.  End function
58. Define main method
59. Input "Enter link" , n
60. Input "Press 1 for Encryption and 2 For Decryption", ch
61. If (ch==1) then
62. Let res=Encryption(n)   //Calling function to encrypt the link
63. Print("Encrypted link" ,res)
64. Else if(ch==2) then
65. Let res=Decrypted(n)  // Calling function to decrypt the link
66. Print("Decrypted link" ,res)
67. Else
68. Print ("Invalid choice")
69. End main method
70. End class
```

References

1. Garrison, G., Kim, S., Wakefield, R.L.: Success Factors for Deploying Cloud Computing. Commun. ACM. 55, 62–68 (2012).
2. Herhalt, J., Cochrane, K.: Exploring the Cloud: A Global Study of Governments' Adoption of Cloud (2012).
3. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.
4. Hashizume, K., Rosado, D. G., Fernandez-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 5.

5. Rebollo O, Mellado D, Fernandez-Medina E, Mouratidis H. Empirical evaluation of a cloud computing information security governance framework. Inf SoftwareTechnol2015;58:44–

6. McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley Professional.

7. Howard, M., & LeBlanc, D. (2003). *Writing Secure Code*. Microsoft Press.

8. Khan, A. N., Zhang, X., Alam, M., & Ali, S. (2013). A cloud manager architecture for high availability and load balancing in cloud computing. *Information Sciences, 252*, 77-87.

9. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security, 13*(2), 113-170.

10. Gupta, A., Gupta, D., & Gupta, H. (2016). Secure coding practices for cloud computing: A comprehensive survey. *Journal of Cloud Computing, 5*(1), 1-18.

11. Sharma, R., & Chen, L. (2017). Secure coding in cloud environments: An empirical study. *Journal of Systems and Software, 134*, 222-239.

12. Mell P, Grance T. Version 15 The NIST definition of cloud computing October 7. National Institute of Standards and Technology; 2009http://csrc.nist.gov/groups/SNS/cloud-computing.

13. Maddineni, V. S. K., &Ragi, S. (2011). Security Techniques for Protecting Data in Cloud Computing. Electrical Engineering.

14. Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing.In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1, pp. 647-651).IEEE.

15. F. Sharif and A. Hafeez (2012). The Analysis of Cloud Computing Major Security Concerns & their Solutions, Journal of Information & Communication Technology, pp. 48-53

16. Yogesh L. Simmhan, Beth Plale, and Dennis Gannon. 2005. A survey of data provenance in e-science. ACM SigmoRec. 34, 3 (2005), 31–36

17. Joseph Ricci, Ibrahim Baggili, and Frank Breitinger. 2019. Blockchain-based distributed cloud storage digital forensics:Where's the beef? IEEE Secur. Priv. 17, 1 (2019), 34–42