INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Adoption of Cloud Enabling Cyber-Security Model in Organizations

Ali Zaheer Agha[1,2]*, Rajesh Kumar Shukla[3], Ratnesh Mishra[4], Ravi Shankar Shukla[5]

1 Research Scholar, Invertis University, Bareilly, Uttar Pradesh, India
2 Assistant Professor, Computer Science & Engineering department, Dr.Rizvi College of Engineering, Kaushambi, Uttar Pradesh, India
3 Professor & Dean, Faculty of Engineering & Technology, Invertis University, Bareilly, Uttar Pradesh, India
4 Sr. Assistant Professor, Department of Computer Science and Engineering, BIT Mesra, Patna Campus, Patna, Bihar, India
5 Assistant Professor, Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Saudi Arabia

OPEN ACCESS

Received: 12-08-2022
Accepted: 29-10-2022
Published: 27-12-2022

Citation: Agha AZ, Shukla RK, Mishra R, Shukla RS (2022) Adoption of Cloud Enabling Cyber-Security Model in Organizations. Indian Journal of Science and Technology 15(48): 2727-2739. https://doi.org/10.17485/IJST/v15i48.1592

* **Corresponding author**.

alizaheer7@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To carry out a systematic review on Cloud Computing (CC) security problems in order to suggest a cyber-security model for a secure CC environment. **Methods:** ResearchGate, PLOS One, MDPI, Wiley, Springer, Scopus, IEEE Xplore, IOP Conf. Series, and TechScience Press are used as sources in this research. Cloud security, risks to CC, issues with the current models, and the proposed model are among the significant keywords included in this article. Analysis and evaluation of the cloud computing security models have been conducted on the basis of factors like the technology used, authorization, security level, malicious insiders, VPN, encryption, etc. **Findings:** After doing comprehensive study of the previous models, it was analyzed that the client service provider's (CSP) are focusing on their own security but not of client's security. One problem is that there is no real set of standards to measure cloud security. Encryption key should be known to client only. Also, clients are not aware of security policies of CSPs. Furthermore, to overcome some issues certification programs should be there for CSPs so that clients are able to judge the CSPs according to their needs. Lastly, periodical awareness programs should be conducted for both CSP and client employees. **Novelty:** In this research a security model is proposed in which it is tried to implement solutions to various threats like hacking, unauthorized access of data, data encryption and authentication. It has proposed to develop a Cyber Security Model (CSM) for improvement of security features of cloud when it is used by organizations. In this study features like Single Sign-On for users to get proper authorization; key supervision is used for encryption of data and VPN controller is implemented to guard data from hackers have been added.

Keywords: Cloud Computing; CyberSecurity; Cloud Security Challenges; Data Protection; Security Model

1 Introduction

Cloud Computing (CC) is an internet-based service and that facilitates for sharing computer resources along with other devices on user demand. It is a mechanism to enable 'on demand' shared resources [1]. The computing resources are pooled over a cloud that can be provisioned to the users when they need them. The users will be charged only for what they consumed from the cloud. This facilitates the small and medium scale businesses by reducing the capital expenditures of deployment of the resources at sites [2]. The security and privacy of data is one of the major concerns in CC [3]. Data leakage will be due to a lack of security controls when the cloud service provider (CSP) does not offer sufficient data protective solutions. This might lead the customer to lose a lot, pose a security concern, and frequently result in security breach [4]. Various security checks must be deployed to maintain CC security and prevent data breaches [5].

Many organizations are concerned about handing over control of their essential apps and historical databases containing sensitive data to a CSP. To eliminate this problem, CSPs must guarantee that their clients' applications and sensitive information are protected and controlled in the same way as on-site systems are. To do so, CSP should explain to a customer that almost all service levels are fulfilled and that audits can ensure adherence. The objective of this research is to identify as to what extent the different types of risks influence CC adoption decisions and accordingly, proposes a conceptual adoption framework.

A lot of research has been done and published in the field of cloud security for different parameters. In Ref. [6] Bnasod et. al. stated that they are developing Anticrime portal where they will upload data in encrypted mode onto cloud. The users can use and study over this data by decrypting it only after two-way authentication is successfully proceeded. Anticrime branch maintains huge data related to criminals and crimes done. They use manual system to maintain individual file. They need a space to maintain these files digitally. So, cloud is the best solution for it and that to be maintained with security. They discussed the different techniques like cryptography that are used for secure data storage on cloud. For future, they stated to utilize cryptography to maintain data in encrypted format and will use 2-way security to authenticate users of this anticrime branch data. Similarly, in [7], author presented a solution to some security issues of cloud computing. They provided the benefits and effectiveness of security in cloud computing. Also, their model provided security and scalability of data sharing for users on the cloud computing. For future work they proposed that the model shall be implemented over medical data records. New solutions of other threats and attacks can be found for its sensibility and importance. The performance and efficiency of the cloud-computing environment can be improved. One drawback of this model is that no VPN controller is present which helps to protect and hide users IP address from hackers. In another research [8], the authors have suggested a big new/up-to-time security architecture for cloud-based computing domain which includes two factor authentication, AES based file encipher and decryption of data uploaded on cloud, admin verification and locking of users, fetching IP details of users is stored in one database & encryption/decryption details is stored on different database. Overall work deals on enhancing security for cloud computing, they suggested working on representation so that hacker/attacker cannot easily fetch information from the cloud databases and load their corrupted files as he requires to get access all the database data centers, which is very tough and hard to breach or crack. All these attacks which could be performed on the previously implemented system could be reduced to zero enhancing the security of the cloud and at the same time identifying and servicing only the genuine clients. Moreover, in article [9], Lubna discussed about the CC security and stated that it's an essential aspect of computer security, and it poses a major challenge to its widespread adoption because the fact that CC services are essentially based on Internet connection makes them vulnerable to a variety of attacks and security threats that may result in either light or severe impacts. Lubna reviewed the significant attacks threatening the security of CC; moreover, she provided solutions and possible countermeasures to serve as a reference for comparative analysis. In Ref. [10], author evaluated IT users experience and perceptions with regard to security towards existing or new cloud-based solutions by using survey methods. This article determined the IT users' acceptance and risk awareness rate in regard to cloud security. It illustrated the view of CSP's actions and assessment of the CC services provided by them to the IT users. Mubarak mentioned that the future research work will carefully analyses some of the major security threats to the cloud services based on the security threat analysis produced by Cloud Security Alliance (CSA). In Ref. [11], Kashukeev introduced a new CIA triad data security model. It added a three-factor authentication (3FA), as well as a Single sign-on using the OpenID standard. Thus, the effectiveness of preventive control is increased. The model focused on data security and protection. Furthermore, Ivan mentioned that the proposed model will significantly increase data security in cloud technologies and thus reduce the risk of misuse and misuse of personal data, as well as the misuse of identity. Cyber threats and cyber-crimes will be reduced. The use of smart technologies will be safer and psychological stress and distrust in consumers will be reduced. In another work [12], the authors investigated a key issue related to security that can be considered as a threat is those cloud service providers have to share resources between their customers, so to achieve a satisfactory security level they should update their security policies based on their customer profiles. This survey highlighted in start different cloud computing models which could be deployed followed by security issues related to cloud computing, out of those research challenges security related to securing data is the most key objective that should be accomplished under each deployed model. Securing network

access to provide virtual access under cloud computing is another fundamental concern in cloud computing. This survey paper highlighted all those security issues and the work cut out for the improvement so far.

To sum up, the previous survey publications in cloud computing security are not thorough enough. They don't really address the security of host, network, application, and data levels of cloud platform. Not all customer and service provider opinions are taken into account in some studies. Our suggested approach differs in that it conducts a thorough study of the problems that existed at all levels of the cloud computing infrastructure. After that, it talks about the current fixes for these problems. The survey concludes by highlighting the unresolved problems and challenges and providing suggestions for further study. An overview of various recent studies looking at security threats, attacks, as well as issues in cloud systems can be found in Table 1. It describes the research papers currently available in cloud infrastructure for the years 2019 to 2020. Additionally, it shows the papers' deficiencies.

Table 1. Summary of existing surveys

References	Objective	Focus of work/ advantage	Limitations
(6)	Data storage security	• Secure data storage on cloud • Cryptography to maintain data in encrypted format • Use 2-way security to authenticate	• No innovative mitigation approach used • The number of categories used in the reviewed taxonomy is very limited.
(7)	Data protection over CC	• Identity threats on cloud data • Enhancement of encryption of data • OTP used as login technique	• Few criteria used to evaluate the reviewed techniques • The encryption techniques are still not fully mature and face many problems
(8)	Identity based authentication	• 2-factor based authentication • AES based file encryption • Admin verification	• Very limited details mentioned in the paper related to review literature • Poor quality of graphics used
(9)	Survey on cloud security	• Survey study on CC • Address different threats & attacks • Existing solutions to such attacks	• The paper is a general survey. It does not propose countermeas ures for each area. • Limited to a qualitative assessment of cloud security threats.
(10)	Determine user acceptance & risk awareness towards cloud security	• Analyze major threats to CC • Evaluate IT user experience • Illustrate CSP' action & assessment of CC services	• The number of reviewed papers is very less • The paper is a general survey, it does not propose countermeasures for each area.
(11)	Data security model in CC	• Introduce 3-factor authentication • Add Single-SignOn using OpenID • Focuses on data security	• No innovative mitigation approaches • Few criteria used to evaluate the reviewed techniques
(12)	Analysis of Security issues in CC	• Analyze threats in CC from service providers perspective • Offers best practices to providers for better control • Allows providers to define & enforce policies to protect data	• The paper is a general survey, it does not propose countermeasures for each area. • This is a theoretical paper and does not provide any proper solution to reduce the security risk.

After reviewing many research articles, we analyzed that the cloud environment must be secured in an efficient, effective, and low-investigation way. To achieve so, we believe that the primary aim of our research is to be the development of an autonomous & cloud-enabled Enhanced Cyber Security Model (CSM) for organizations in terms of a form suite to commercialize threats against malicious hackers, along with cyber attacker activity.

Part two of this article covered cloud service & deployment models in general. Third section looked at cloud security concerns as well as attacks. Mitigation strategies against cloud security lapses were covered in Section four of the paper. Eventually, the findings and research directions were provided.

2 Methodology

Online databases such as Science direct, Scopus, Google scholar, Springer, and IEEE explore were searched to get relevant studies for this research. This study reviewed around 25 research papers from leading information systems journals and conferences. The articles were searched and ordered based on the categories of risks in adopting cloud-computing services such as technical, legal and operational risks.

2.1 Service Models

Infrastructure-as-a-service (IaaS) is the core for other layer; platform-as-a-service (PaaS) is a stage for developing as well as hosting users' application; and software-as-a-service (SaaS) is a layer that typically functions as a service on demand. Figure 1 shows the service models in CC.

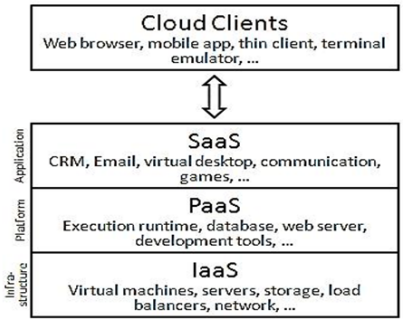

Fig 1. Cloud Computing Service Model

1. **Software-as-a-Service (SaaS):** SaaS (Software as a Service) is a subscription-based service that allows customers to access software kept on a public cloud & supplied via Internet, such as online office apps and e-mail clients. Users can manage their requirements for a cheap cost by subscribing to an online software solution instead of purchasing new software. Customers rely on service providers to keep them safe. SaaS may not always necessitate the usage of particular hardware or software, but it does need a constant Connection to the internet.
2. **Platform-as-a-service (PaaS):** The PaaS layer, which sits just beneath SaaS, enables developers to quickly design, build, and deploy SaaS software applications. PaaS is a reliable choice for programmers as it concentrates on designing and executing apps rather than merely managing the platform. Usually, service providers have complete control over the system that the developers use.
3. **Infrastructure-as-a-service (IaaS):** IaaS, the lowest level, serves as a platform for the layers over it. IaaS includes networking devices, workstations, system software (OS), including storage. This enables customers to view all contents without having to purchase additional equipment. As there is no need to purchase or maintain the core technology, IaaS might be the most reliable and quicker solution for executing tasks; nevertheless, because it is depending on Internet access, reliability is a top priority.

2.2 Deployment Model

The National Institute of Standards and Technology (NIST) have suggested four main deployment models for cloud computing: public clouds, private clouds, hybrid clouds. Figure 2 mentions various types of deployment models in CC.

2.2.1 Public Cloud

Hardware / software products are managed transparently between many customers in a public cloud. As they are maintained and operated by a 3rd party cloud service provider, these clouds are excellent for insensitive data.

2.2.2 Private Cloud

A private cloud is operated by an organization, and almost all of the cloud's infrastructure and technologies are just available from within that company's boundaries. This cloud is usually incredibly expensive, though it's significantly safer than a public cloud because the company manages all equipment administration and repairs.

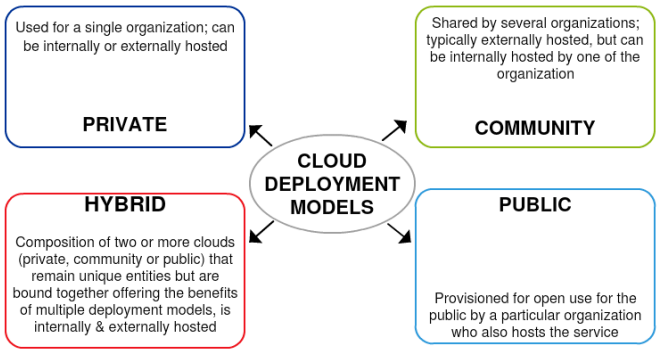

Fig 2. Cloud Computing Deployment Models

2.2.3 Hybrid Cloud

A hybrid cloud (for instance – a public–private cloud) combines different cloud kinds. Since it integrates the advantages of the associated clouds, such type of deploying design allows for maximum adaptability, as well as a lot of data distribution options. This cloud is managed from a single place.

2.2.4 Community Cloud

Community cloud is a cloud infrastructure that allows systems and services to be accessible by a group of several organizations to share the information. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

2.3 CC Security Issues and Challenges

Organizations face the same security risks and challenges in cloud computing that they do in traditional computer environments, at a high level. Unlike traditional data centers, however, handling cloud services requires distributing duty for risk and security management with the cloud supplier. This extra level of difficulty brings with it several exceptional safety issues and challenges that are only seen in the cloud.

Here is a list of five most significant security issues that organizations face while implementing cloud computing:

2.3.1 Unauthorized Access

PaaS and SaaS systems benefit from the ability to deploy on-demand services via self-service tools. It does, however, raise the chances of unauthorized use. When services & features are supplied or used without IT's awareness, organizations are particularly vulnerable.

Employees who have access to cloud - based information through the use of various cloud devices like computers, laptop computers, as well as tablet pcs can sometimes implement the outside security issues, presenting cloud computer technology security challenges for businesses, especially when personnel carelessness as well as authorization breaches may be involved.

2.3.2 Reduced Control and Clarity

While moving toward a cloud platform, organizations may lose lots of traceability because the cloud provider takes on all of the responsibility for policy and design. The scale of the authority transfer will be defined by the cloud storage service model(s) utilized, such as SaaS vs. PaaS vs. IaaS, as well as an absence of complete visibility can result in a variety of businesses, cloud-based privacy & vulnerabilities exist. Security breaches, data redundancy, as well as inefficient supervision could compromise the security of cloud content, diminishing the effectiveness of security controls. Such risks can be avoided by putting in place safety procedures, which monitor data and identify unusual user behavior. The most widespread cloud security problem that organizations encounter is a lack of visibility.

2.3.3 Unsecure Interfaces and APIs

They can contribute to the resolution of cloud - based security problems. APIs are required for a personalized cloud understanding; however, they also pose a security risk. APIs enable businesses to personalize cloud service features to their own requirements. It also has encryption, access, and data recognition capabilities.

Poorly designed APIs are more likely to be exploited, resulting in data breaches of privacy. While Interfaces are beneficial to developers, they can also pose security issues if not carefully examined for bad design and security. However, adequate activity tracking using access management could assist in the detection of any insecure interfaces and APIs.

2.3.4 Systems Security problems

Cloud infrastructure networks are more vulnerable to system failures since they are complex and rely on third-party support. Vulnerable flaws render systems unsecure, allowing hackers to exploit security flaws and steal valuable data. Security breaches, like insecure systems as well as shared memory & tools, are at the root of several cloud-based security constraints. These could act as entrance points for malicious assaults and as portals for big data thefts.

2.3.5 Breach, theft or disclosure of Information

The simplicity of data sharing in the Cloud is a big asset and important to working in the Cloud. However, data theft, deletion, and leaking are all major risks.

The CC makes sharing the data which is stored there quite straightforward. However, the information is available publicly, a privacy breach is often a risk Information can be easily transmitted with others using cloud-based networks, whether through a public URL or direct response requests. There are technologies that can simply scan the Web for insecure cloud distributions that could constitute a data security concern.

2.3.6 Malware Injection

Hackers take use of data centers to inject malicious software. Hackers have access to personal data when malware is installed on cloud servers. This is a big problem in cloud systems.

2.3.7 Distributed Denial-of-Service (DDoS) Attacks

When cloud computing was in its beginnings to acquire popularity, no one would have considered DDoS attacks. Attacking cloud solutions was difficult at first, but the widespread usage of computers and cell phones has allowed DDoS attacks more possible.

2.3.8 Accounts Hijacking

The rate of account hijacking is growing at a much faster rate as cloud computing becomes more popular. Staff can log onto their accounts from a variety of devices, permitting hackers to steal sensitive data on the cloud from distance. Furthermore, hackers have the right to alter this data. Reused passwords and programming flaws are two other kinds of hijacking. All of these actions provide attackers access to sensitive information, allowing them to modify or waste it.

2.3.9 Social Engineering Assaults

Because workers and supervisors have access to the cloud, and anyone may access data from anywhere, social engineering and phishing scams are possible. Hackers will be able to enter the systems from almost anywhere if you keep your account logged in. In order to take precautionary actions, staff and top executives has to be informed of phishing & social engineering attempts.

2.3.10 Insider Threat

Many organizations remain not concerned about insider dangers. Employees can exploit the accounts, allowing hackers to get access to the cloud-based systems. Whether they're doing on purpose or by accident, it may have a huge negative impact on an organization. As a result, we can't overlook internal risks in addition to external threats. The main obligation of cyber-security pros & staffers would be to pay close attention to what they're doing don't let fraudsters retrieve the information. Figure 3 [13] graphically shows kinds and volume of the threats that happened in organizations in the last 12 months.

3 Results and Discussion

The several benefits of CC have earlier been shown. Yet, a large number of scholars express grave cautions about security and privacy concerns. Hence, offering practical and effective answers to CC adoption's hazards might aid in its success. The following recommendations can help minimize the risks connected to CC.

Fig 3. The Actions Taken to Prevent or Minimize Cyber-Security Risks in the UK, 2019

3.1 Guidelines to Reduce Risks in Cloud

3.1.1 Avoiding Cost and Vendor Locks

Due of ongoing expenses and fees associated with switching to some other cloud, clients frequently assume a bad view about Cloud adoption. The majority of ongoing expenses are connected to the services and supporting infrastructure. Higher leadership should thus choose the best CSPs.

3.1.2 Clear and Defined Technical Contract and Service Level Agreement (SLAs)

The agreements stipulating the specific duties and obligations between both the CSPs and customer should be in-depth. To prevent further legal disputes, it must act as a legally valid technical document for both entities.

3.1.3 Outsourcing and Authorization of Data

To prevent overlapping data ownership and privacy concerns, it is essential to specify which portions of the content belong to the supplier and which portions to the customer. The cloud-stored data is supposed to only be accessible by authorized users.

3.1.4 Developing Trust, Improving Security, and Using Software and Applications

Between the many CSPs, trust is necessary. Since a lot of data is transferred daily to the cloud, CC firms have to ensure that the content does not get into the wrong hands. Only the client and service providers need to share the security and privacy related to the use of software and equipment.

3.1.5 Leadership preferences and knowledge gaps

Decisions to utilize CC are determined by the policies that legislator's draught. Making incorrect adoption decisions may result from having insufficient knowledge about and an inadequate comprehension of CC technologies. These decision makers, such as higher leadership, frequently lack an IT background, which limits their knowledge of the newest technology. This increases the risks associated with adoption decisions for CC.

3.1.6 Bandwidth, Data Integration, and Disaster Recovery

Data integration and bandwidth risks are shared by customers and service providers. The customer is responsible for making sure that the information is updated on a regular basis, and the service providers are responsible for ensuring the continuity and availability of the data regardless of network failures. Additionally, it is the client's obligation to have high-speed internet for continuous connectivity to the cloud.

Figure 4 [14] shows some measures many organizations plan to take in order to avoid cyber security threats and improve data security in cloud.

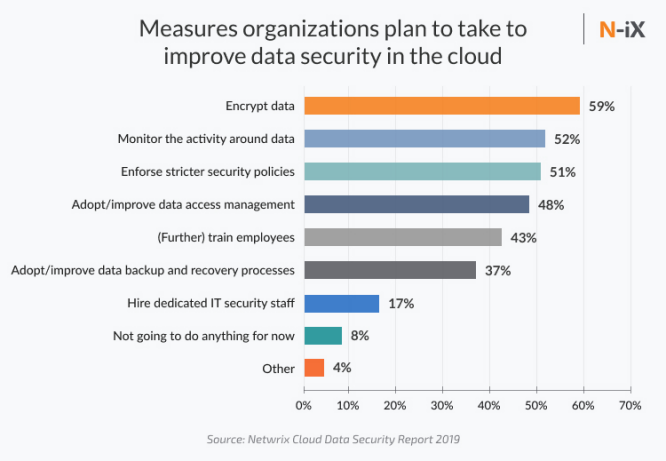

Fig 4. Measures to avoid cyber security threats

3.2 Problems in the Existing Data Security Models

Information protection and the integrity problems have been a major and difficult component of cloud. This section explains potential shortcomings of the current information security model then shortly outlines the proposed cyber-security model for enterprises using cloud computing. There are many constraints in the implementation of cyber security by the organizations which are mentioned in Figure 5 [15].

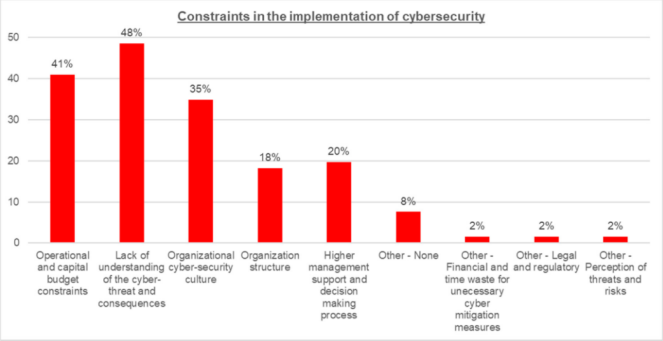

Fig 5. Constraints in the Implementation of Cyber security in Organizations

3.3 Comparative Analysis of Cloud Computing Security Models

In Table 2, we have shown the performance comparison of the system between traditional security methods currently used and our proposed method. In this analysis, a number of important security factors are taken into account, including authorization, technology employed, security, malicious insiders, authentication, encryption, and accountability. There are currently insufficiently detailed survey articles on cloud infrastructure security. They do not address CC security at certain levels. Several published studies have one or perhaps more level restrictions. Additionally, not all customer and service provider opinions are taken into account in some studies. Our proposed model is different, such that it conducts an extensive review of issues that faced all levels of cloud computing infrastructure with a proper analysis of such issues. Then, it discusses the existing solutions used to mitigate these issues. Finally, the survey highlights the open issues and challenges, and gives directions for future research.

Table 2. Comparitive analysis withprevious cloud security models

Continued on next page

Table 2 continued

	Bnasod et. al.[6]	Sauber et. al.[7]	Sanjay et. al.[8]	Kashukeev[11]	Proposed CSM
AUTHORIZATION METHOD	2-WAY SECURITY	OTP	OTP	3FA	RBAC
TECHNOLOGY USED	WINDOWS AZURE	CAPTCHA	NA	SAML, OPENID	SPML
SECURITY LEVEL	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH
MALICIOUS INSIDERS	MORE	LESS	MORE	LESS	LESS
3RD PARTY AUTHENTICATION	NO	NO	NO	NO	YES
VPN USED	NO	NO	YES	NO	YES
ENCRYPTION USED	YES	AES & RSA ALGORITHM	AES ALGORITHM	SSL	YES
ACCOUNTABILITY AND AUDIT	NO	NO	NO	NO	YES

To reduce the data security risk and to improve the cloud security of data in organizations, a cloud-based cyber-security model (CSM) for organizations should address the above issues and add the following security features:

- Use Individual Login and 3rd Party Authenticator for users;
- Use strong Identity Check to restrict unauthorized users;
- With the assistance of Key Supervision, CSM should make sure that the information is encrypted by using robust cryptographic techniques;
- VPN controller for secure and protected access, hide private information, provide network scalability and reduce support costs
- Ensure file integrity

3.4 Proposed Cyber Security Model (CSM)

In this portion, we'll go over a cloud computing security architecture which emphasizes flexibility as well as vulnerability protection. The model is depicted in Figure 6 , and so it is up of various security components.

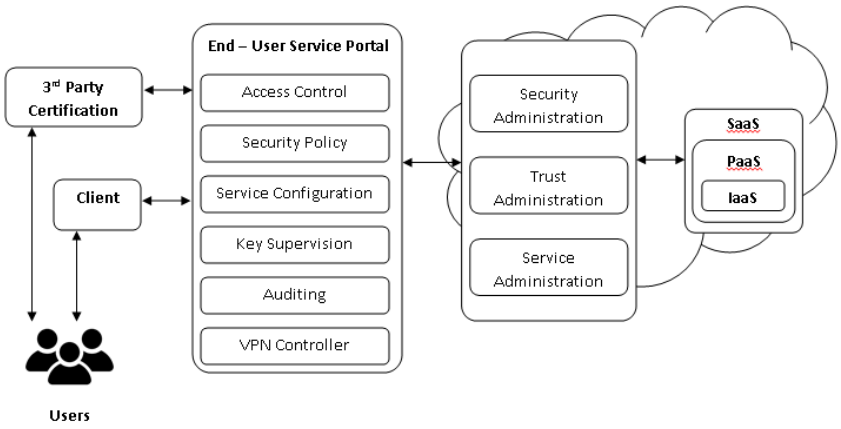

Fig 6. Design of Proposed CSM

The user can be certified by a 3rd Party Authenticator, and then the Customers Gateway can issue a token for service. After signing up for the gateway, users can purchase and use cloud services from a single supplier. Secure access check via Virtual Private Network (VPN) and cloud Service Administration and Utility Framework is provided by the Customers Gateway, which is made up of Access Check, Security Policy, Key Supervision, Utility Framework, Evaluate, and VPN Controller.

3.5 Framework of CSM for Organizations

The framework for the CSM is indicated in Figure 7 that is focused on the security model that defines the attributes of every element and implements the appropriate security techniques for deployment among elements in CC.

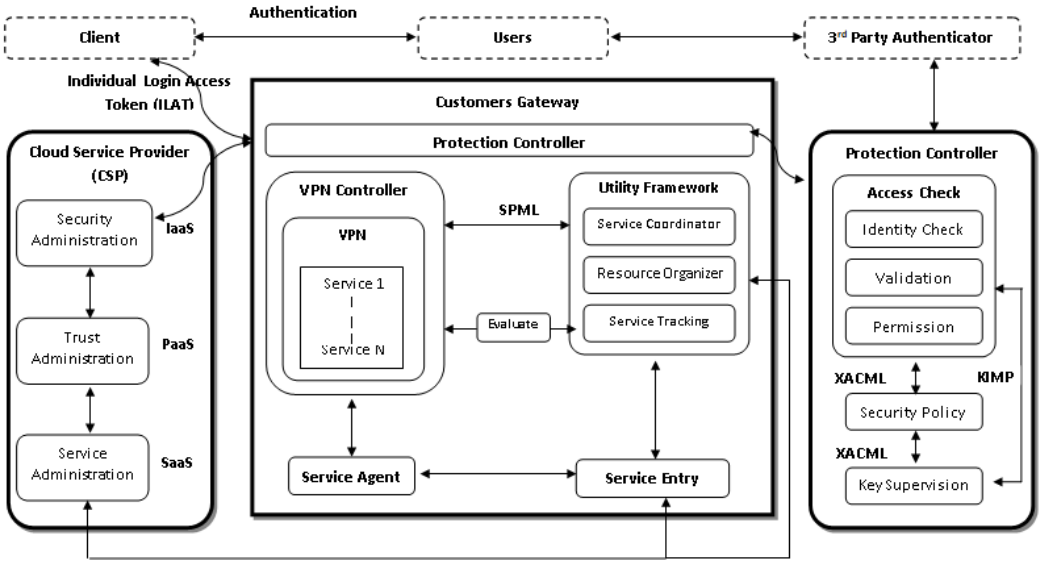

Fig 7. Proposed Framework of CSM

In this model, user can be certificated by the 3rd Party Authenticator, then can be issued token for Customers Gateway. After joining the Gateway, users can purchase and use cloud services which are provided by cloud service providers. Customers Gateway which is composed of Protection Controller, Utility Framework, VPN Controller, Evaluate, Service Agent and Service Entry provides secure access check using VPN and cloud service administration and framework. Using inter-process communication and open APIs, a Resource Organizer in Utility Framework could organize & initialize virtualization technology.

- **Client:** Customers Gateways multifactor authentication allowed users to access the client side from a variety of devices such as a laptop, mobile phone or PDA. Customer can connect to their own cloud using the client-side gateway. Authentication based on a variety of elements, including verification from a 3rd Party Authenticator.
- **Customers Gateway:** When permission is granted, an Individual Login Access Token (ILAT) could be issued based on the user's certification. The Access Check elements then share user information related to Security Policy and validation with several other elements within Customers Gateway and cloud providers via XACML[16] and KIMP[17]. Users may use services regardless of the constraints imposed by service providers.
- **Individual Login (IL):** Users have multiple profiles using various providers, each with its own unique id and password. As a result, the vast majority of network users choose to use the same password everywhere they can, raising security issues. The inconvenient nature of numerous authentications not only reduces user productivity but also increases administrative overhead. Individual Login (IL) technology is being seriously considered by businesses to combat the password issue since it promises to reduce various network and application passwords to just one. To tackle this difficulty, enterprises could employ Individual Login (IL) for cloud consumer to simplify security administration and create better authenticity inside the cloud. This allows users to log in once and access numerous apps and services in the cloud computing environment, allowing for strong user authentication.
- **Utility Framework:** Depending upon the person's account, the Service Agent develops a custom cloud service. The CSP's Service Administration receives this person's account in combining client service composition requirements. To share a user's profile, the SPML[18] can be utilized. The Resource Organizer sends a request to the CSP for tailored resources based on the user's profile SPML and configures the service through VPN.
- **Service Entry, Service Agent:** A Service Entry maintains network services including VPN in the entire process of a Service Agent.

- **Cloud Service Provider (CSP):** A cloud service provider, or CSP, is a business that provides cloud computing components like IaaS, SaaS, and PaaS. CSPs offer cloud computing-based technology & gateway solutions to customers using their own data centers and compute resources. Several pay-as-you-go membership approaches are generally used to charge cloud services. Users are only billed for the services they use, like the period of time customers use a service or the amount of storage capacities they utilize. In the case of SaaS products, cloud providers can either serve and supply their own managed services to users or function as a third-party running an enterprise application.
- **Service Tracking:** Automated service tracking technologies are sometimes used to assure a strong level of service reliability and stability. The suggested security framework ensures a safe connection and makes it easy for users to use cloud services. To give a smooth experience for users, we explore cloud management environments and Individual Login Tokens. In addition, we analyze cloud - based technologies that are available.
- **Protection Controller:** The security control element protects Access Check, Security Policy, and Key Supervision from potential risks. The Access Check module's purpose is to support providers with their user access needs. Based on the specifications, different access checking models might be used. Role Based Access Control (RBAC)[19] is largely viewed as the best access checking model due to its easy, agility in addressing evolving needs, plus assist for idea of minimum authority & effective access administration. RBAC is also policy-independent, able to grab a broad variety of policy needs, and ideal for the policy integration needs outlined before. RBAC is also used towards usage control that extends the reach of access control through inserting prerequisites in access privileges. People should meet the standards in order to be granted accessibility. Because of very volatile nature of cloud, responsibilities & constraints are essential decision considerations for stronger and better restrictions on cloud resource utilization.
- **Security Administration:** The security administration component is responsible for defining and enforcing security and privacy policies. The authentication and identity management module is in charge of identity verification as well as services based upon identities & attributes.
- **Trust Administration:** It's really challenging to combine specifications trust agreement techniques using fine access checking systems in the cloud. The truthfulness must be linked to the service since the cloud is a service-oriented platform. The idea is that once a CSP expands its offerings, a larger sense of trust is required. Additional problem is that we do need to establish bilateral faith in the cloud. So, users must have confidence in the service providers which they select, and providers ought to have faith in the customers to whom they offer their services. Develop a trust administration strategy that contains a generic set of trust negotiation parameters, is linked with service, and is bi-directional. Because the dynamics of cloud service composition are so complicated, trust and access check frameworks should be included.
- **3rd Party Authenticator:** An impartial 3rd party authenticator verifies that a company's goods or services perform as promised. Usually authenticating authorities need an evaluation that for goods will provide an analysis of sample results, continued by recurrent checks plus auditing to ensure that the package's functionality remains consistent. Because the authentication is dependent on regular checking, 3rd Party Authenticators nevertheless need the provider to bear responsibility for what they deliver. As a result, it is not a promise of a specified product's or service's quality.
- **VPN Controller:** A virtual private network (VPN) spreads a company network all over a public network, allowing users to transfer content like if their computers were physically linked to the local network. Increased performance, privacy, & control of the local network are all advantages of using VPNs. This is frequently utilized by telecommuting users to acquire access to resources that are not available upon the public network. While encrypting is widespread, it is not a requirement of a Virtual network. A VPN Controller assists in the creation of many secure connections for clients to securely access server resources.
- **Key Supervision:** The supervision of duties connected with securing, saving, documenting, and organizing encryption keys is known as encryption key supervision. The use of encryption in the organization has risen dramatically as a result of rising security breaches as well as regulatory concerns. A single organization may use variety of new encryption methods, some of which are inconsistent, led to a large number of encryption keys. Every key must be kept, safeguarded, and accessible in a secure manner. Numerous data encryption management standards initiatives are now on-going. Foremost used mechanism is the Key Management Interoperability Protocol (KMIP) that was created by manufacturers then sent to OASIS. KMIP's purpose is to enable users to connect any encryption equipment to a key management platform.

3.6 Security Parameter Comparison

There will be a stronger influence on cloud data security if the proposed approach is put into practise. The system's performance when implemented without security, the typical security techniques already in use, and our suggested solution are compared in Table 3 below. Here, the comparison is calculated based on a number of important security factors, including availability, confidentiality, security, and reliability.

Table 3. Security Parameter Comparison

Security Parameters	Performance		
	Without Security	**Current**	**Proposed**
Authentication	No	Single / 2-way	Double
Availability	Low	High	High
Confidentiality	Low	Moderate	High
Security	Low	Moderate	High
Reliability	Low	High	High

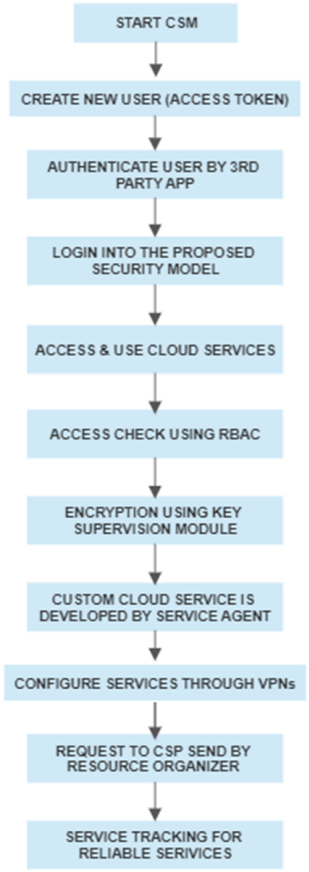

Fig 8. Flowchart of the Proposed Cyber Security Model

4 Conclusion

This study has proposed a framework to find solutions to some critical problems in CC relating to authorization of data by adding Individual login token (ILAT) and 3rd party authority, security of critical information with the help of utility framework. VPN controller helps secure usage of software and programs, and key supervision for encryption to share information in public domain securely. The present investigation is primarily a theoretical in nature; hence, extensive research will be carried out in the future to evaluate the value of the suggested model in identifying hurdles to cloud computing adoption. Future research should focus on the rapidly growing domain of cloud computing and studying the security threats and prescribing appropriate measures and solutions to overcome.

5 Acknowledgment

Each author contributed to the creation and timely completion of this paper. Research and comparative analysis were carried out by A.Z. R.S.S. provided concepts and principles that helped to produce the outcomes. The findings were examined and the paper was updated by R.M. and R.K.S. The final manuscript was finalised by all writers.

6 Authors Research Contributions

- A.Z.A. and R.K.S. conceived of the presented idea.
- A.Z.A. developed the theory and performed the computations.
- R.S.S. and R.M. verified the analytical methods.
- R.K.S. encouraged A.Z.A. to investigate about the current threats in cloud computing and supervised the findings of this work.
- All authors provided critical feedback and helped shape the research, analysis and manuscript.

References

1) Ahmed I. A brief review: security issues in cloud computing and their solutions. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2019;17(6):2812. Available from: http://doi.org/10.12928/telkomnika.v17i6.12490.
2) Dinesh K, and DNG. Cloud Computing and its variable techniques in obtaining data security parameter. *Journal of Engineering Sciences*. 2022;13(1).
3) Amalarethinam G, Josephine DRS. *A Survey on Security Challenges in Cloud Computing*. 2019;24.
4) Sibai E, Rayane&gemayel N, &bouabdo, &demerjian JJ. A Survey on Access Control Mechanisms for Cloud Computing. *Transactions on Emerging Telecommunications Technologies*. 2019. Available from: https://doi.org/10.1002/ett.3720.
5) Sharma, Pradeep. Review Of Cloud Computing Data Security And Threats. *International journal of creative research thoughts*. 2022;10(1).
6) Bnasod N. Implementing Data Storage Security in Cloud Computing. *IOSR Journal of Engineering*. 2019;9(5):68–71.
7) Khalil A, Mostafa, Sauber, Amr M, El-Kafrawy, Passent M, et al. *A New Secure Model for Data Protection over Cloud Computing*. 2021. Available from: https://doi.org/10.1155/2021/8113253.
8) Sanjay, Jafri, Syed, Nigam N, Gupta N, Gupta G, et al. A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing. *IOP Conference Series: Materials Science and Engineering 748 012026*. 2020;748. Available from: https://doi:10.1088/1757-899X/748/1/012026.
9) Alhenaki L, Alwatban A, Alamri B, Alarifi N. A Survey on the Security of Cloud Computing. *2nd International Conference on Computer Applications & Information Security (ICCAIS)*. 2019. Available from: https://doi:10.1109/CAIS.2019.8769497.
10) Almutairi MS. Cloud Computing: Securing without Losing Control. *Journal of Advances in Mathematics and Computer Science*. 2019;p. 1–9. Available from: https://doi.org/10.9734/jamcs/2019/v31i230106.
11) Kashukeev I, Denchev S, Garvanov I. Data security model in cloud computing. *Data security model in cloud computing*. 2020;5(2):55–58. Available from: https://stumejournals.com/journals/i4/2020/2/55.
12) Dashti W, Qureshi A, Jahangeer A, Zafar A. Security Challenges over Cloud Environment from Service Provider Prospective. *Cloud Comput Data Sci*. 2020;1(1):12–20. Available from: https://doi.org/10.37256/ccds.112020318.
13) The Most Taken Actions by Businesses in Order of Preventing or Minimizing Cyber Security Risks, 2019 . 2019. Available from: https://www.digitalmarketingcommunity.com/indicators/preventing-minimizing-cyber-security-2019/.
14) Netwrix Cloud Data Security Report, 2019 . 2019. Available from: https://www.netwrix.com/2019cloudsecurityreport.html.
15) Progoulakis I, Nikitakos N, Rohmeyer P, Bunin B, Dalaklis D, Karamperidis S. Perspectives on Cyber Security for Offshore Oil and Gas Assets. *Journal of Marine Science and Engineering*. 2021;9(2):112. Available from: https://doi.org/10.3390/jmse9020112.
16) OASIS, "eXtensible Access Control Mark-up Language(XACML)" . . Available from: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.
17) OASIS, "Key Management Interoperability Protocol (KMIP)" . . Available from: http://docs.oasis-open.org/kmip/spec/v1.2/os/kmip-spec-v1.2R-os.html.
18) OASIS, "Service Provisioning Mark-up Language(SPML)" . . Available from: https://www.oasis-open.org/standard/spml/.
19) Role Based Access Control (BRAC). . Available from: https://docs.microsoft.com/en-us/azure/role-based-access-control/overview.