iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56670

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

Authentication Authorization and Security Issues in Cloud Computing

Subhankar Sarkar[1], Salini Roychowdhury[2]
[1]*Ph.D. Enrolled, Dept. of CSE, MAKAUT, Haringhata, Nadia, West Bengal, India*
[2]*Assistant Professor, ACE Engineering College, Ghatkesar, Telangana, India*

Abstract: ***Cloud Computing is basically a technology used to store and access data and Cloud Computing is a technology that is growing day by day. One of the reasons for the growth of this technology today is that it can be accessed from anywhere with just a computer device and the internet. But here lies the security risk of user data. so, it is necessary to ensure the security of information for the user. user data security can be ensured through the authentication and authorization process. Allows the user to access the cloud platform after verifying the user's identity through an authentication and authorization process. This authentication and authorization method can reduce the data risk of cloud computing users. In this paper, we have tried to show the data risk aspects of cloud computing users and the possible solutions. We will also try to describe the data protection and security aspects of cloud computing.***
Keywords: Cloud Computing, Security Risk, Authentication, Authorization.

I. INTRODUCTION

Cloud Computing is an internet technology where users can store and access data from anytime anywhere if an Internet Connection and Computer Device are required. Here users can Store and manage data on remote servers. Cloud computing is always changing because it is being updated technically. There are also several different autonomous management domains that exist on the network, and the multi-institutional nature of cloud computing can pose risks and threats. due to the existence of multiple autonomous domains in a virtual organization, the situation becomes much more complicated. A lot of research has been done in cloud computing to ensure that user data is protected from this situation but we have yet to reach that level till now. In a situation necessary for the evolution of role-based access control. Cloud computing is a Virtual organization-based technology or environment. So naturally, there are different domains. Access should therefore be controlled using global management and local autonomy for users. Authentication is used to ensure security in cloud Computing It uses both side client and server, and the user can use it only with the permission of the server. The authorization technique allows users to log in. That is to give the user the ability to access.

Authentication is a term used to protect users in cloud computing, basically, Authentication is a process where a user has to prove his identity to a server or client. In this case, a user is already registered with the server or client, and that user is required to use his username and password for authentication, often at intervals. The authentication process is used on both the client and the server.

Authorization is the name given to a process of granting permission to a user to do or access something. That is a process of checking whether the user has the necessary permissions to use that resource. Since the authorization here allows the user to access information only after authentication, the system here knows who is accessing the information. Again, the user is not always required to get permission to access the information available on the internet. Such as the various information available for studies available on various websites.

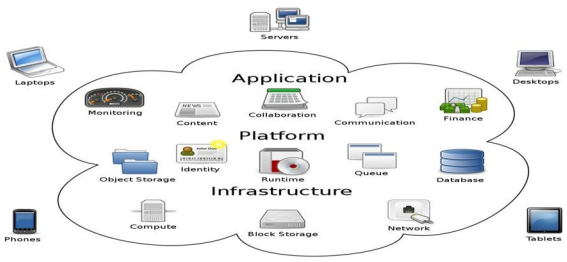


Figure-1. Cloud Computing Architecture.

II. LITERATURE REVIEW

1) A New Security Mechanism for Vehicular Cloud Computing Using Fog Computing System 2019. here, MhidiBousselham, Nabil Benamar, and Adnane Addaim show, Here is basically a work on vehicular cloud computing (VCC) that can do the computational work of vehicular shooting in a very interesting way. Traditional cryptographic algorithms are shown here but security needs to be ensured after compromising the keys located here. Also, fog computing architecture is used here to ensure a stable vehicular network. Also, a new DT technology and UBP are implemented as an alternative solution for data protection privacy in vehicular cloud servers. Decoy files are provided here in such a way that attackers cannot tell the difference between real and fake files.
2) Authentication and Authorization in Cloud: Reviewing The Trend Pratiba D, Dr. Shobha G, Arjun A R V College of Engineering Bangalore, Karnataka, India. This paper mainly discusses the various aspects of authentication and authorization in cloud computing. Also, this paper focuses more on user authentication in cloud computing. Also, several issues and risks in using cloud computing have been highlighted. Besides the authentication and authorization of cloud computing to access any user data, the issue of trust has emerged as an important issue. Besides, the use of timing to protect its data is mentioned here that is, the user can access this data at a certain time, but after that time, the user is not allowed to access the data.
3) User Authentication Issues In Cloud Computing Mrs. S. M. Barhate, Dr. M. P. Dhore. This paper highlights the issues of file sharing between users or data files that are vulnerable to attack. Also described are security privacy challenges with interoperability with data stored in the cloud. Also, unauthorized users may break in and pose a security risk to the data. It also mentions the use of virtual machines in different situations and assigned to cloud users to access data stored in the cloud. Also in this paper, User Authentication. Workload Migration. Data Migration. Workload Management are discussed. Also includes a detailed discussion of user authentication and various authentication techniques used in cloud computing. Besides, various risk aspects of cloud computing along with possible solution methods and various algorithms are discussed in this paper.
4) A New Framework of Authentication Over Cloud Computing Megouache Leila, Zitouni Abdelhafid, and Djoudi Mahieddine. In this paper, various aspects of cloud computing are first discussed in detail. Also, identify the risk aspects of cloud computing including several topics Different threats of cloud computing are highlighted along with concepts of authentication and authorization. Besides highlighting the various threats of cloud computing. Several aspects of the proposed security model are shown here viz Virtual private network, Access with authentication, the algorithm used to encrypt data and AES.
5) Enhancement of Cloud Authorization System Using Predicate Logic Sandeep Saxena, Goutam Sanyal, and Shashank Srivastava. Here the whole topic of cloud computing is covered as well as authorization, prediction logic, and authorization rule sets. Although this paper mainly discusses authorization techniques, the. The hierarchical structure of Objects and Resources based on Access Permission and derivation of the authorization rule is highlighted in the proposed model. Apart from the optimization of rule sets, various algorithms are used here. Also used is the authorization rule syntax tree The Propose Model also uses generic architecture for the Propose Authorization Framework.

III. CLOUD COMPUTING

Cloud computing is a service through which multiple computing services including server storage, database, and networking software analysis are provided over the Internet.
Now, first of all, we need to know the cloud computing overview.

A. *Types of Cloud Computing*

Basically there are four types of cloud computing according to the requirements, respectively-

1) *Public Cloud:* Public Cloud is a medium open to all users. Where the user can use this platform by paying a small amount. here the user can collect and access data on this platform through the internet. A cloud service provider manages and operates the public cloud. It is maintained by the public cloud service provider, and it is accessible by the general user so the number of users is also unlimited.
2) *Private Cloud:* When an organization uses cloud computing technology to store and manage its own data, it is called a private cloud. Alternatively, it can be called internal Cloud or Corporate Cloud. As it is used by third parties to build their own data center. i.e., private cloud technology used only for a single user or single organization. The biggest advantage to users here is low cost and maintenance by public cloud service providers.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

3) *Hybrid Cloud:* Hybrid Cloud is the creation of a single IT environment that consists of multiple environments connected through local LANs (Local Area Networks), MANs (Metropolitan area Networks), VPNs (Virtual Private Networks), and APIs. In other words, a hybrid cloud is a combination of public and private clouds This means that some of the applications and data are hosted on a private cloud that is owned and managed by a company, while other applications and data are hosted on a public cloud that is managed by a third-party provider. The benefit of a hybrid cloud is that it allows companies to take advantage of the scalability and cost-effectiveness of a public cloud while still maintaining control over sensitive data and applications.
4) *Community Cloud:* When allowing systems and services to be accessed by a group through different organizations to share information within a specific group. on the other hand, is a type of cloud that is shared by multiple organizations with common concerns, such as compliance requirements or security concerns. These organizations collaborate to build and maintain the community cloud and share the resources and costs associated with it. The benefit of a community cloud is that it allows organizations to take advantage of the benefits of a shared cloud while still maintaining control over their own data and applications.

B. Cloud Computing Service

1) *Software as a Service (SaaS):* SaaS or software as a service is commonly known as on-demand service or on-demand software. Here basically the cloud service is provided according to the needs of the user through software. The user only needs a computer device, an internet connection, and a web browser to use this Service.

SaaS features respectively
It is mainly operated from a central location and accessible to remote servers through the Internet.
If any software updates are required, it is done automatically. The user does not have to.
For the user to use this Cloud service, the service provider has to pay some amount and accordingly, the services are purchased on a usage basis.
Examples: Salseforce.com (On-demand CRM solutions) Google Apps (Gmail, Google Calendar, Docs. etc), GoToMeeting (Video conferencing software) etc.

2) *Platform as a Service (PaaS):* PaaS or Platform as a service creates and provides an environment to run any program. Or it can be also said that it is a platform made for the run time environment for programmers. That is, it allows programmers to create various web applications for testing here. Another advantage here is that the user can purchase the used applications from the cloud service provider on a per-use basis. Usually, the tools provided by PaaS cloud service providers are respectively Programming Languages, databases, application frameworks, and other tools.

Examples: Google App Engine (Cloud storage client library), Azure (Security, IoT), salesforce (RM services, Sales Cloud, Mobile Connectivity), etc.

3) *Infrastructure as a Service (IaaS):* Infrastructure as a service or IaaS is an important part of cloud computing. Here customers use Internet technology according to their own needs or provide basic computing, network, and storage resources after paying over the Internet. In short, it is a cloud-based pay-as-you-go service. IaaS has three categories in this model respectively Public, Private, and Hybrid. A private cloud usually means that the infrastructure is owned by the customer. On the other hand, in the case of the public cloud, the platform used by the cloud computing user resides in the vendor's data center. A hybrid cloud is essentially a combination of public and private clouds, and here the customer chooses the best of the two.

Examples: Amazon Web Service (Elastic, Elastic Compute Cloud (EC2) MapReduce, Virtual Private Cloud, etc.), Reliance Communications (Reliance Internet Datacenter), Tata Communications (Insta Compute), etc.

C. Cloud Computing Applications

Cloud service providers offer a variety of applications in many cases. Among them, the most used cloud computing applications are respectively-
(a) Art Applications, (b) Business Applications, (c) Data Storage Applications, (d) Education Applications, (e) Management Applications, (f) Social Applications, (g) Entertainment Applications.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

1) Art Applications

Art Application Cloud computing offers these applications for quick design of cards, and images or to design anything easily. Several cloud art applications respectively-

a) *Moo:* Moo is one of the cloud art applications, commonly used to design and print a variety of business cards, mini cards, and postcards.

b) *Vistaprint:* The Vistaprint cloud computing application lets you easily design a variety of Printed marketing materials. such as business cards, Booklets, wedding invitation cards, etc.

c) *Adobe Creative Cloud:* The Abode Creative Cloud application is primarily designed for creative professionals, this is a suite of apps that includes a variety of image editing programs like Photoshop, Illustrator, XD, Dreamweaver, etc. Which is useful for creative professionals.

2) Business Applications

Basically, a business application cloud service is a cloud computing service based on service providers. This service is always available to users. Several Business Applications respectively-

a) *MailChimp:* MailChimp basically it is an email publishing platform, It provides different template designs and saving options when sending emails.

b) *Salesforce:* Salesforce is generally a platform that provides tools for e-commerce, sales, service, business service, etc. Also provides a cloud development platform for various business services.

c) *Chatter:* Chatter basically helps to share important information about organizations in real time.

d) *Bitrix24:* Bitrix24 is a cloud platform that provides communication management and social collaboration tools. It is mainly a collaboration platform.

e) *Paypal:* Paypal is the easiest online payment service in cloud computing. It mainly collects payments through credit cards, debit cards, and Paypal account holders online.

f) *Slack:* Full form of SLACK Searchable Log of all Conversations and Knowledge. It basically helps users to create public and private channels for communication.

g) *Quickbooks:* The QuickBooks cloud platform is essentially an enterprise run anytime, anywhere on any computing device. It allows multiple users to work together on the same system at the same time.

3) Data Storage and Backup Applications

Generally, cloud computing allows us to store various types of information and access it with the help of Internet connections. Many times, the data stored in the cloud is lost or the cloud provider is responsible for providing security, so offers various recovery applications to recover the lost data. Data storage applications used in the cloud respectively-

a) *Box.com:* Box generally provides an online environment for collaborating on secure workflows. Various types of files like word excel power point pdf images etc can be saved here. The main advantage of using a cloud computing box is the drag-and-drop service available for files.

b) Mozy: Moji is a service to provide a powerful online backup solution for all users' personal and business data.

c) *Joukuu:* It provides the easiest way to share and track backup files that are cloud-based. Many users use cloud-based Joykuu to search files, folders

d) *Google G Suite:* Google G Suite is one of the best cloud storage and backup applications available today This includes tools for managing cloud storage and cloud apps It also includes services like Google Calendar, Docs, Forms, etc. One of the most popular apps now is Gmail which offers free services to its users.

4) Education Applications

Currently, cloud computing is a very popular service in the world of education. It offers various online distance learning platforms and various information portals for students. In education, one of the major advantages of using the cloud for students is that it provides a powerful virtual classroom environment, easy availability and secure data storage, and a scalability environment.

a) *Google Apps for Education:* Google Apps is the most widely used free platform for educational work. The most common uses here are web-based email, calendaring, and document storage which is useful for studying.

b) *Chromebooks for Education:* One of the most important projects for educational purposes is the Google Chrome book, It is designed to enhance innovation in education.

c) *Tablets with Google Play for Education:* It allows educators to implement technology solutions in the classroom, and make them available to students.
d) *AWS in Education:* It generally provides education friendly environment in schools, colleges, and universities.

5) *Entertainment Applications*

Here a multi-cloud strategy is used to communicate with the audience. Cloud computing provides entertainment applications such as video conferencing or online games.

a) *Online Games:* Cloud gaming is one of the most important forms of entertainment today. It is an online game service that can be run from the cloud from a remote location. Here are the best cloud gaming services right now GeForce Now, Vortex, Project xCloud, PlayStation Now, etc.
b) *Video Conferencing Apps:* Nowadays video conferencing apps are an important means of communication, By using cloud-based video conferencing apps we can communicate with our friends and relatives instantly. By using video conferencing, costs are reduced, efficiency is increased and interoperability is eliminated.

6) *Management Applications*

This platform typically provides administrative control over a variety of applications and infrastructure. Here is basically a management tool offered by cloud computing. Some important management applications are below-

a) *Toggl:* it helps in tagging the time allotted for any particular project.
b) *Evernote:* Evernote allows us to sync and store basically any of our recorded notes or typed notes in one convenient location for free.
c) *GoToMeeting:* It provides Video Conferencing and online meeting apps, We can start meeting with our business partners anytime from anywhere using mobile or tablet. Not only that, here we can join the meeting in seconds, and we can view the presentation on the sharing screen.

7) *Social Applications*

Social cloud applications basically allow a large number of users to connect with each other using social networking applications. Currently, there are several popular social cloud applications namely-

a) *Facebook:* Facebook usually uses cloud storage to allow users to share photos, videos, statuses, etc. with their friends and relatives. We get a notification when some friends like or comment on a post on Facebook.
b) *Twitter:* Twitter is currently a popular social networking site and microblogging system. From here users can follow high-profile celebratory friends and relatives and get news. Not only that, a short post called Tweet can be made here.
c) *LinkedIn:* LinkedIn is a social networking site, especially for students, and professionals.

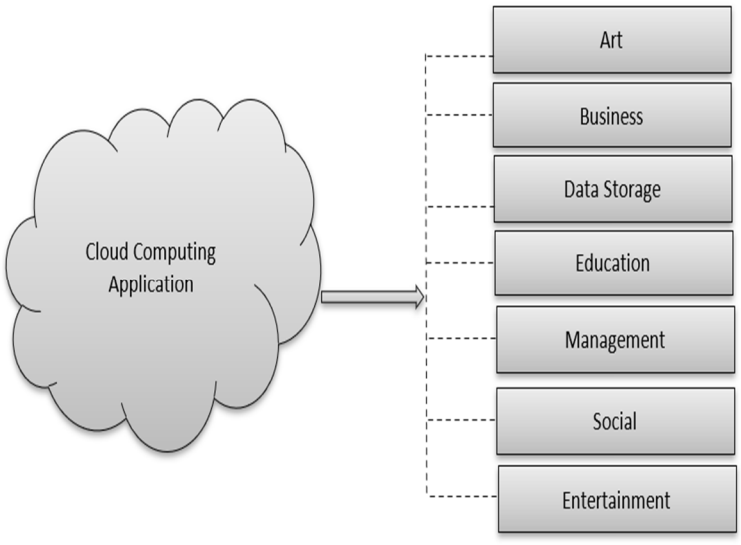


Figure-2. Cloud Computing Applications.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

IV. SECURITY RISKS OF CLOUD COMPUTING

Cloud computing has several advantages such as accessibility, mobility, Storage capacity, etc. Again, there are security risks in cloud computing. I will discuss several cloud security risks in this paper.

Data Loss: Along with the benefits of cloud computing, there are also security risks, the main one being data loss. this is what we know as Data leakage. Data loss is a process where user-stored data is usually deleted or destroyed or unreadable by a user, or software applications. The biggest data loss in cloud computing occurs when any of our stored sensitive data gets into the hands of another user. As a result, no operation can be done on one or more of the stored data, the hard disk drive does not work properly.

1) *Hacked Interfaces and Insecure APIs:* Cloud computing is a service dependent on the Internet. So, APIs used by external users should be secured first. In the case of cloud services, most are communicated through APIs, which is a simple way. Some of these services are available in the public domain of cloud computing. The major disadvantage of these cloud services is that they are accessed by third parties, so these services are easily vulnerable to hackers.
2) *Data Breach:* Data breach refers to when any confidential data is viewed or accessed or stolen by a third party without authorization. Here user data is hacked by hackers.
3) *Vendor lock-in:* One of the biggest security risks in cloud computing is vendor lock-in. Basically here, when a service is transferred from one organization to another these organizations face various problems. As there are different platforms offered by different companies, it can be difficult or sometimes difficult to move from one cloud to another cloud.
4) *Increased Complexity strains IT staff:* Migrating or managing cloud services is a complex matter for IT staff. That's why IT staff need the skills to maintain cloud data management.
5) *Spectre & Meltdown:* Spectre & Meltdown, programs are allowed to view and steal processed data on the computer. As these personal computers can run on the mobile cloud, as a result, they can store important confidential information such as passwords, personal information, photos, email business documents, etc. in the memory of running programs.
6) *Denial of Service (DoS) attacks:* A Denial of Service or DoS attack occurs when the system has too much traffic to buffer the server, just in case. In these cases, the main targets of the DoS attackers are large corporate servers such as the banking sector, media companies, and government organizations. Not only this, attackers charge time and money to recover lost data.
7) *Account Hijacking:* Account hijacking is a major and serious security risk in cloud computing today. Here, hackers steal important personal information of users or organization information Like bank accounts, email, social accounts, etc. And with that, hackers use other accounts to carry out unauthorized activities.

V. AUTHENTICATION IN CLOUD COMPUTING

Authentication is a term used to protect users in cloud computing, Authentication is a process through which it is understood who is using the data stored on the server. That is a process of granting permission to the user to use the data stored on the server. That is, when the user uses any information on the server through authentication, it is checked whether he is the real user before that. And after confirming that the user is allowed to access the server.

There are various types of authentication methods which are discussed below –

1) *Single-Factor Authentication:* Single-factor authentication or SFA is one of the simplest forms of authentication. The most popular form of SFA is username and password-based authentication. Nowadays there are many applications that are using SFA as their primary authentication method. The password authentication method here relies on mutual confidentiality between the user and the online service provider.
2) *Two-factor Authentication:* Two-factor Authentication 2FA is one kind of multi-factor authentication process that requires two methods to verify identity. Similarly, we can say it is a two-step verification process which is for the verification of identity. like as Name and Password or OTP (One-time password) based verification before login. This 2FA Authentication method protects the user's login and data from various unwanted attacks or data theft.
3) *Multi-factor Authentication:* When the user has to go through multiple verification processes it is called multi-factor authentication. Here, since the user has to go through several verification steps, it is a key component of strong identity and access management policies. in the case of MFA, having additional verification mechanisms greatly reduces the number of changes to a successful cyber-attack.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

Famous Authentication techniques are: -

a) *Password-based Authentication:* Password-based authentication is the simplest way of authentication technique here a specific password is required for the particular user, when logging in, the password and username match the information in the database stored on the system. Then it will be successfully authenticated.
b) *Passwordless Authentication:* In the case of the Passwordless authentication technique, no user password is required for login. As a result, the user does not need to remember the password here. Here instead an OTP (One-time password) is issued to the user's mobile number or email id through which the user log in. In a word, it can be called OTP (One Time Password) based authentication.
c) *2FA/Two-factor Authentication:* Two-factor authentication is a higher-level authentication and access management (IAM) policy, here two methods are required to verify user identity. Additional PIN or security questions are asked for this user so that it can authenticate the user.
d) *Single Sign-on:* Single Sign-on SSO Session and user authentication service where to access multiple applications the user is allowed to log in once time. Like one login ID one password This process the risk of forgetting the user's password and improves the security.
e) *Social Authentication:* The Social Authentication technique is a multi-step authentication technique where users can log in such as Facebook ID, Google ID, or Twitter ID. This method can be called logon. because the user does not have to upload information while logging in here, login is possible with the information used by social media.

VI. AUTHORIZATION IN CLOUD COMPUTING

Authorization is the process by which a user is granted permission to do or access something. That is a process of checking whether a user has the necessary permissions to access something on the server. That is, the authorization process is a second process to allow access to data after authentication. In other words, in simple terms, this process allows a user to access data.

Various Authorization Techniques are:

1) *Role-based Access Control:* RBAC is the control provided according to user profiles or user roles in an organization. That is, users are given role-based access control skills according to the importance of their work. It is used or implemented for system to system or user to system.
2) *JSON web Token or JWT:* JWT or JSON web token is an open standard object, that is used to transmit data securely. Here data is transmitted between authorized users and the data is usually in the form of objects.
3) *Security Assertion Markup Language:* Security Assertion Markup Language or SAML provides authentication certificates between service providers and it is an open standard. Certificates issued to users are digitally signed. which are exchanged through XML documents.
4) *Open ID Authorization:* Open ID Authorization authenticates clients and then helps verify the identity of end users.

VII. POSSIBLE SECURITY SOLUTION IN THE CLOUD

So far, we have discussed various aspects of cloud computing including security risks and authentication and authorization, we will know about possible security solutions for cloud computing risks-

1) *Identity and Access Management (IAM):* Identity access management is an important aspect of security systems in many areas, including cloud computing. It can be applied through both authentication and authorization fields. Identity Access Management basically ensures that the user is a legitimate user. Users can then access the stored data from the server. That is, here the user is allowed data access only after complete confirmation.
2) *Security Information and Event Management (SIEM):* SIEM is one of the approaches to reduce data security risks in cloud computing. SIEM security management Cloud-based platform is generally designed for security purposes, mainly to help with data collection and data monitoring and analysis. Since in cloud computing, SIEM works as a stand-alone solution, we can consider it as part of the data security suite.
3) *Cloud Access Security Broker (CASB):* CASB is a set of cloud computing security solutions that provide control and visibility. That is, the CASB is usually an organization or point of enforcement between the cloud service provider and the user receiving the cloud service, either on-premises or cloud-based. The CASB method is used to ensure data security, control the use of devices or cloud applications, or protect against threats to stored data.

4) *Cloud Data loss prevention (CDLP):* Cloud Data loss prevention protects or helps to protect sensitive data stored on cloud servers. Not only this, CDLP also protects sensitive data from being stolen or destroyed.
5) *Extended Detection and Response:* XDR is an important method in cloud computing because XDR has multiple layers of security for data stored in the cloud. It can generally be called a tool or integration endpoint in cloud computing. It provides increased visibility and analysis and feedback across workloads or user networks

Apart from these, there are several methods of cloud security solutions-

- Secure Access Service Edge (SASE).
- Security Service Edge (SSE).
- Security Incident and Event Management (SIEM).
- Cloud Workload Protection Platforms (CWPP).

VIII. CONCLUSION

In this paper we mainly discussed various aspects and details of cloud computing, security and risk aspects of cloud computing were also discussed. Authentication and authorization issues are also discussed in detail. And we also discussed in this paper Possible security solutions in cloud computing. Several potential cloud security solutions are also pointed out. Next, we will try to work on the security of cloud computing and especially work on authentication techniques, In order to ensure the security of future cloud platform user information and user access using one or more authentication methods.

Authors' contributions: Mr. Subhankar Sarkar wrote the main manuscript, and Miss Shalini Roy Chowdhury also contributed to writing and reviewing references for this manuscript. Mr. Sarkar discusses Cloud Computing and Cloud Computing applications and security risks. And Miss Roychowdhury discussed the possible solutions to the risks of cloud computing. Review of Previous Papers on Authentication and Authorization in Cloud Computing, and Conclusion written by Mr.Sarkar and Miss Roychowdhury.

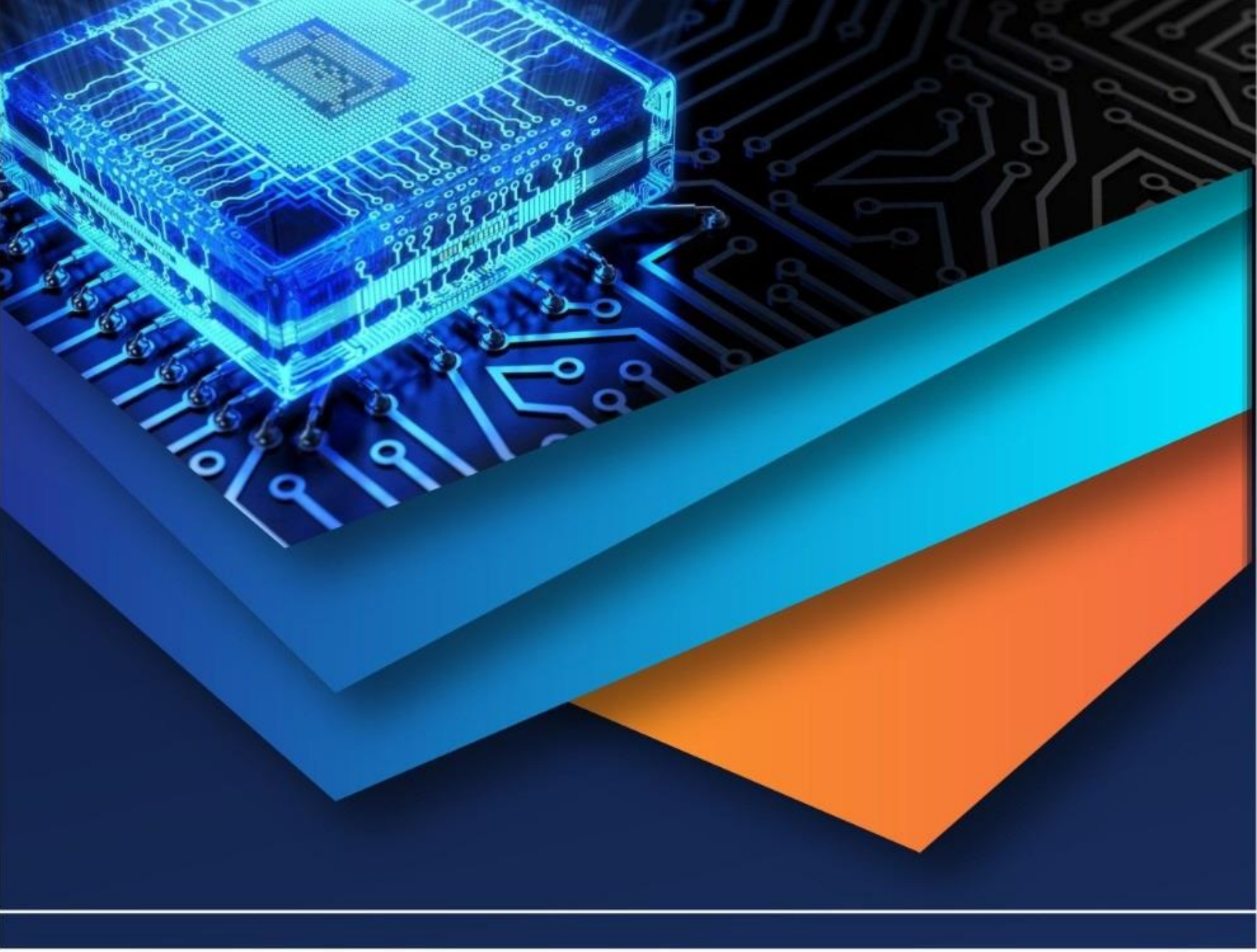
REFERENCES

[1] Cloud Computing and Types of Cloud Service: https://www.knowledgehut.com/blog/cloud-computing/what-is-cloud-computing#what-is-cloud-computing.
[2] Cloud Computing and Cloud Computing Index: https://www.tutorialspoint.com/cloud_computing/index.html
[3] Cloud Computing Applications: https://www.javatpoint.com/cloud-computing-applications
[4] Security Risk of Cloud Computing- https://www.javatpoint.com/security-risks-of-cloud-computing.
[5] Cloud Access Security Broker: https://www.netskope.com/security-defined/what-is-casb
[6] Security information and event management (SIEM): https://www.mimecast.com/blog/what-is-cloud-siem/#:~:text=A%20cloud%20SIEM%2C%20or%20security,of%20a%20broader%20security%20suite.
[7] Cloud Data loss prevention: https://cloud.google.com/dlp
[8] Cloud Security Solutions and XDR: https://www.exabeam.com/explainers/cloud-security/cloud-security-solutions-8-solution-categories-you-must-know/
[9] Authentication and Authorization in Cloud: Reviewing The Trend 1 Pratiba D, 2 Dr. Shobha G, 3 Arjun A 1,2,3 R V College of Engineering Bangalore, Karnataka, India. IJCSN International Journal of Computer Science and Network, Volume 3, Issue 6, December 2014 ISSN (Online): 2277-5420 www.IJCSN.org
[10] A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System Mhidi Bousselham Ibn Tofail University ENSA Kenitra, Morocco mhidi.bousselham@uit.ac.ma Nabil Benamar The Graduate School of Technology Moulay Ismail University Meknes, Morocco n.benamar@est.umi.ac.ma Adnane Addaim Ibn Tofail University ENSA Kenitra, Morocco adnane.addaim@uit.ac.ma Conference Paper · April 2019 DOI: 10.1109/WITS.2019.8723723
[11] A New Framework of Authentication Over Cloud Computing Megouache Leila1, Zitouni Abdelhafid 1 , and Djoudi Mahieddine2 Lire Labs, Abdelhamid Mehri Constantine 2 University, Ali Mendjli, 25000 Constanine, Algeria {leila.megouache, abdelhafid.zitouni}@univ-constantine2.dz 2 TECHNE Labs, University of Poitiers, 1 rue Raymond Cantel, 86073 Poitiers Cedex 9, France mahieddine.djoudi@univ-poitiers.fr
[12] User Authentication Issues In Cloud Computing Mrs. S. M. Barhate1, Dr. M. P. Dhore2 1 (shwetab73@yahoo.com, Dept. Of Electronics & Computer Science RTM Nagpur University, Nagpur, India) 2 (mpdhore@rediffmail.com, Dept. Of Electronics & Computer Science RTM Nagpur University, Nagpur, India). IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 30-35 www.iosrjournals.org
[13] Enhancement of Cloud Authorization System Using Predicate Logic Sandeep Saxena1, Goutam Sanyal2, and Shashank Srivastava3 Asst. Prof.,1Krishna Engineering College, Ghaziabad, India Research Scholar, 1National Institute of Technology, Durgapur, India 3MNNIT Allahabad, India saxena.s.in@ieee.org, Shashank12march@gmail.com International Journal of Security and Its Application Vol.11, No.1 (2017), pp.245-256 http://dx.doi.org/10.14257/ijsia.2017.11.1.20
[14] Cloud Computing Authentication Techniques: A Survey DR. V. V. S. S. S. BALARAM Professor & HOD, Dept of IT, Sreenidhi Institute of Science and Technology, Ghatakesar, Hyderabad, TS, India. ISSN 2319-8885 Vol.06, Issue.03 January-2017, Pages:0458-0464. www.ijsetr.com
[15] Cloud Computing Security Issues and Its Challenges: A Comprehensive Research Jaydip Kumar. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019.
[16] Authentication and Authorization Mechanism for Cloud Security J. Vijaya Chandra, Narasimham Challa, Sai Kiran Pasupuletti. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019.

AUTHORS DETAILS

1. Mr. Subhankar Sarkar, Corresponding Author- B.Tech & M.Tech in CSE, B.ED-Pedagogy of Mathematics. A.D.F.M. & P.G.D.F.S.E - Fire & Safety. Presently Ph.D. Enrolled at - Dept. of CSE, M.A.K.A.U.T- Haringhata, Nadia, W.B. India. Research Interest- Internet of Things, Cloud Computing, Machine learning. Email- elinksuvankar.sarkar@gmail.com

2. Miss. Salini Roychowdhury Co-Author, B.Tech & M.Tech in CSE, Presently Assistant Professor- Dept. of CSE. at ACE Engineering College, Ghatkesar, Telangana. India. Research Interest-Machine learning, Artificial Intelligence, Cyber Security, Networking. Email- salinir10@gmail.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY