OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

Fortifying Data Security and Privacy Preservation in Cloud Computing: Challenges and Solutions

Monika Deore[1] , Shweta Bhor [2], Abhisha_Dhamale[3], Aneri Thange[4]

Department of Electronics and Computer Engineering Sanjivani College of Engineering, Savitribai Phule Pune University Pune, India[1,2,3,4]

monikadeore392@gmail.com[1], bhorshweta21@gmail.com[2,], dhamaleabhisha@gmail.com[3], bhorshweta21@gmail.com[4]

Abstract: ***The emergence of cloud computing, which makes it easier to provide a variety of services and resources via the internet, points to a quickly changing technical environment. The flexibility and scalability provided by cloud computing have caused significant changes in data processing, storage, and administration for businesses. Despite its many advantages, however, worries about data security and privacy have become the most pressing issues. The intrinsic ease of use and scalability of cloud technology have highlighted the possible dangers of data breaches, illegal access, sensitive information disclosure, and privacy violations. Thus, privacy and data security are important concerns for users of cloud computing and have a big impact on the hardware and software aspects of cloud architecture. " Reflecting the changing dynamics of cloud computing, this succinct review captures the most common issues, workable solutions, and emerging trends in the field of data security.***

Keywords: Cloud Infrastructure, Cybersecurity, Privacy Safeguards, Data Integrity.

I.INTRODUCTION

The big data term defines datasets with their enormous amounts, varied shapes, and changeable processing velocities. Concurrently, cloud computing, the provision of a range of technological services via the internet, including servers, storage, databases, networking, software, and analytics, enables users to remotely access cloud applications and data from anywhere. This paradigm revolution in data management makes it possible to store and retrieve data from the cloud without the users having to own and maintain physical hardware and software resources. This transformation not only brings undeniable cost savings but also transforms classical data centers from being fixed, resource-hungry configurations into dynamic, pay-as-you-go structures. Cloud storage comes as a better option to traditional storage mechanisms under its on-demand provision of resources, efficient hardware management, and global data availability.

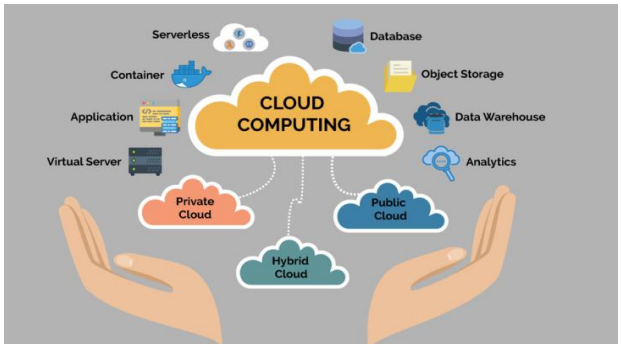

Fig.1.Illustrates the different types of cloud

Some of the major advantages of cloud storage include large storage capacity, secured data protection, effortless remote backup capabilities, and cost-effective scalability. accountability for the supervision and upkeep of the archived information in their centers.

II.CATEGORIZATION OF CLOUD ENVIRONMENTS

The categorization of cloud computing demarcates three major categories: hybrid clouds, personal clouds, and public clouds. Further, the services of cloud computing are generally divided into Platforms as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS).

The "public cloud" refers to computer services provided to the general public by third parties over the Internet, making them available to whoever wishes to use or acquire them. Private clouds, led by companies such as Elastic-Private Cloud, Microsoft, HP Data Centers, and Ubuntu, offer increased security provisions compared to public clouds. Private cloud implementation requires organizations to set up and manage their infrastructure, as well as provide employees with the necessary skill sets. Hybrid clouds combine both the public and private cloud capabilities, creating a heterogenous distributed system. Cloud resources are accessed through a range of service models, including Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS).

Platform as a Service (PaaS): Platform as a Service (PaaS) represents a key component in the gamut of cloud computing, which provides virtual platforms and infrastructure appropriate for application deployment, testing, and development. This revolutionary PaaS model is responsible for passing on the operation of underlying pieces of infrastructure, including operating systems, servers, and networking to cloud providers and thus freeing consumers to focus on the nitty-gritty aspects of programming as well as the development of programs. For organizations with aspirations to speed up the development and deployment cycle, Platform as a Service (PaaS) is an invaluable resource that maximizes efficiency and helps facilitate nimble innovation in organizational environments.

Fig.2 Classification of cloud computing based on the service model

Software as a Service (SaaS): Symbolizes a revolutionary way of accessing business software and web applications, eliminating the need for local installations through the provision of seamless accessibility through web browsers. In this model, cloud providers take total responsibility for controlling all aspects of the software environment, including security measures, maintenance routines, and application updates, together with infrastructure maintenance.

Famous for its ease of use and unprecedented accessibility, SaaS stands out as the go-to option for individuals and businesses looking for ready-to-use software solutions. Ranging from ubiquitous email solutions to powerful office productivity packages and advanced customer relationship management (CRM) software, SaaS solutions cover a wide range of operational needs, enabling users to automate processes and improve productivity with ease.

Infrastructure as a Service (IaaS): Infrastructure as a Service (IaaS) is a cloud computing paradigm in which providers provide virtualized computer resources over the internet. It includes a virtual data center for storing data and is a platform for application development, testing, and deployment. Companies looking for scalability and flexibility with control over infrastructure appreciate IaaS solutions.

The cloud computing market is growing rapidly, with interest from both commercial and educational circles. Despite this, there are still challenges with cloud storage systems, like access limitations and security threats. Cloud computing raises multiple security issues like permission management, confidentiality, integrity, availability, and verification because of the data-sharing nature between users and providers in two ways.

The threat of compromising data is growing, which has been divided into critical and archive data. Subscribers whose usage depends on non-stop access could be affected largely by any delay or loss in critical data. Archival data, being lesser in access rate, yet hold value in between non-critical times. The main focus would thus be toward providing untroubled access to critical information, whereas problems of security and reliability would have to be targeted in cloud storage systems.

concerns such as permission management, confidentiality, integrity, availability, and verification due to the nature of two-way data sharing between users and providers.

The risk of data compromise is on the rise, categorized into vital and archival data. Any disruption or loss of vital data can significantly impact subscribers who rely on continuous access. In contrast, archival data, although less frequently accessed, remains valuable during non-critical periods. Therefore, the primary concern lies in ensuring uninterrupted access to critical data while addressing security and reliability issues in cloud storage systems.

III.LITERATURE REVIEW

Venturing into the present scenario of technological developments, including the spread of the Internet Things of (IoT), the development of smart cities, and the digitalization of businesses, highlights the utmost significance of data storage and management solutions. With data volumes swelling, driven by these developments, Cloud storage systems have become vital pillars of the digital age, responding to the growing need for effective data storage and management. This shift to cloud solutions is felt through governments, businesses, and individual consumers, bringing with it a new age of data availability and scalability. But with the promise of prosperity come looming issues about data security and privacy violations, including threats of unauthorized access, data leakage, and privacy invasions. Although previous research has explored some facets of data security and protection of privacy a systematic analysis of these matters in the context of cloud storage systems is still a major void. In this academic project, we undertake an extensive literature review concerning data security and privacy issues of cloud storage system and the resultant countermeasures. Our critique starts with an explanation of cloud storage basics, including its definition, taxonomy, architectural paradigms, and applications in the real world. We then proceed to a detailed discussion of the multidimensional challenges and requirements related to data security and privacy maintenance in cloud storage environments. Lastly, we explain a number of research directions for the future, thus setting a course for better data security in the constantly changing realm of cloud storage systems.

EVOLUTION OF CLOUD COMPUTING: TRACING ITS ORIGINS AND MILESTONES

The origin of cloud computing dates back to the days of , Client-server computing, with centralized storage in which software programs, data and controls are on servers.With businesses growing, the growing need for storage made it compulsory for

users to access servers for data or execute software applications.

The emergence of distributed computing represented a turning point, where linked computers easily pooled resources as and when required, setting the stage for the eventual development of cloud computing.

During a prescient speech given at MIT in 1961, John McCarthy foresaw computers being sold like utilities, where cloud computing worked like a public utility. Though premature, this visionary idea was revived as technology advances made it a reality.

In 1999, Salesforce.com carved a very important entry in the history of real-world computer usage by introducing a website providing downloadable software delivered through the Internet, symbolizing the beginning of a new generation of computing models.

The groundbreaking launch of Amazon Web Services (AWS) in 2002 by Amazon marked a revolutionary change, providing an extensive array of computing, storage, and artificial intelligence technologies that spurred the spread of cloud computing worldwide.

Ever since Microsoft launched Windows Azure in 2008, other prominent players such as Oracle and HP have joined the cloud computing industry.

Google Apps became a company involved in business cloud computing in 2009, emphasizing the mass use of cloud technology.

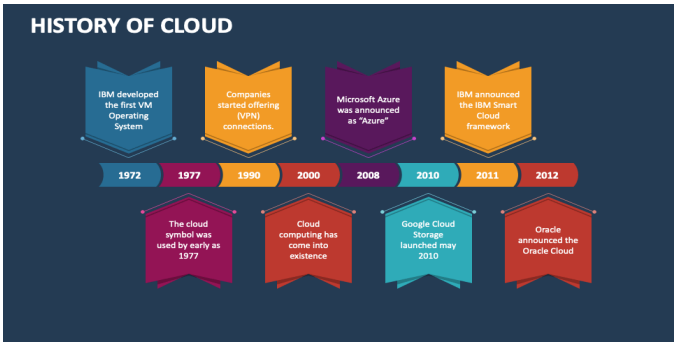

Fig.3.History of cloud computing

Pre-Cloud Computing Challenges :

- Lack of flexibility
- High on-premises costs: The cloud is generally cheaper in terms of on-premises costs. On-premises solutions are at a high cost for hardware and replacements.
- Lower scalability: The scalability of the system or solution for adapting to alterations in the need for computing resources is limited.
- Poor security for data
- Lower collaboration
- Remote access to data is not available.
- Allocate enormous space for servers: Servers and data center hardware require a lot of physical space.
- Lower possibility of data recovery

.

Solutions Post-Cloud Computing :

- No space on the server is required.
- The maintenance of software and hardware doesn't Need specialists.
- Better protection of data.
- Disaster recovery.
- Easy deployment.
- Economical.
- Management of service is easy.
- Efficiency of collaboration.

Fig.4.Top cloud providers

UNVEILING CLOUD COMPUTING ARCHITECTURAL FRAMEWORKS

Technology architecture is a blueprint or design plan that describes how a system or technology is organized, its components, interactions, and data flow. It gives a high-level overview of the organization, design, and development of the system.

Are two of sections of Cloud Computing Architecture are (1) Front End and (2) Rear End

Front End: It provides the interfaces and applications required by the cloud service. Web browsers such as Internet Explorer and Google Chrome are among such applications. Portable devices and clients are supported.

Back End: The back end in cloud computing is the infrastructure that handles the application's core processing, data handling, and execution of the application's functionality

.

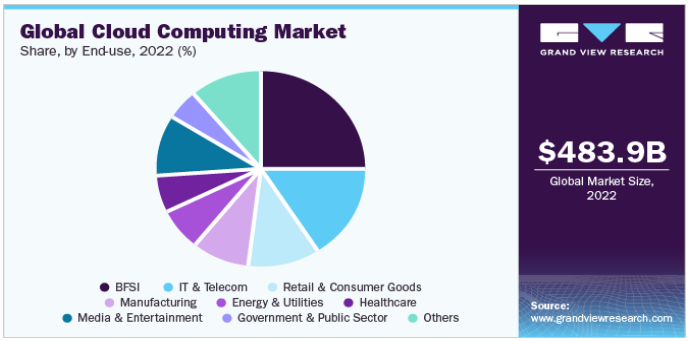

Fig.6.Graph of the global cloud computing market.

All of the programs that execute the application on the front end are managed by it. It has numerous servers and data storage systems.

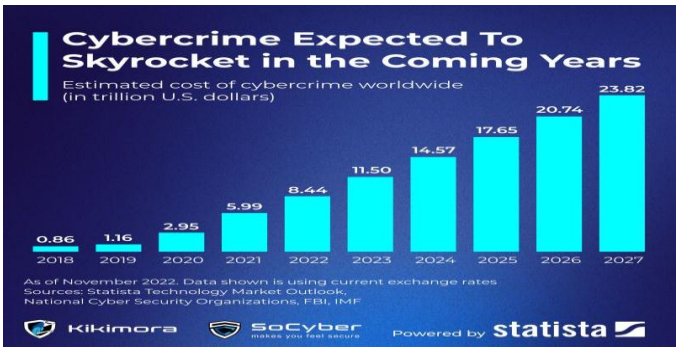

Fig.7.Graph showing the expected rate of cybercrime in the coming years.

The cloud computing market size in 2022 was estimated at USD 483.98 billion. Cloud computing consumption has also gained momentum due to the COVID-19 Pendemic. Increased usage of cloud computing does, however, raise security and privacy concerns that inhibit the growth of the market. Cybercrime's attack surface expands with more devices and systems interconnected through the Internet of Things (IoT) and fifth-generation wireless technologies (5G networks). Cybercrimes might increase as a consequence, specifically those directed toward IoT devices, which are at risk.

As per Cybersecurity Ventures, the price of cybercrime will rise across the world by 15% annually over the next five years to USD 10.5 trillion by 2025.

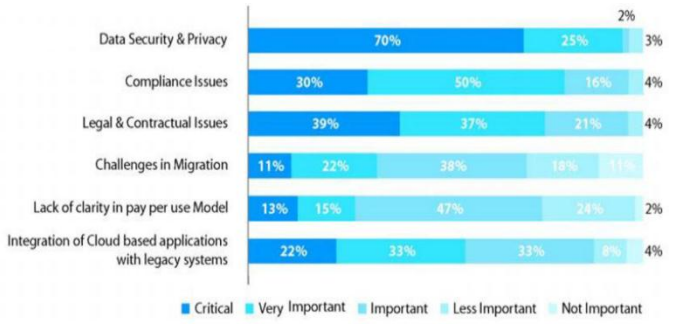

Fig. 8. Data Security and Privacy Challenges- Major Inhibitors to Cloud Adoption

DATA SECURITY CHALLENGES

Cloud computing data security is the collection of practices, technologies, and policies aimed at safeguarding data stored,processed,and transmitted in cloud environments.

Since security threats are constantly in flux and we must keep ourselves current with the most recent issues, the subject of data security issues in cloud computing is a never-ending one. A user is a consumer of cloud computing. Cloud computing users' privacy is increasingly becoming a cause for concern.

There is an endeavor in collaboration to draft a bill of rights to address the problem of user rights. There have been many challenges for data security, most of which are a direct result of our growing reliance on digital technologies and data. The principal problem is that increasingly more businesses are adopting cloud computing. The employment of any device to store and retrieve information from cloud providers' centers poses some security and privacy issues, including data theft, loss, and modification.

Cyberattacks: Flaws are exploited by cybercriminals and malicious actors to gain private information without authorization. A denial-of-service (DoS) attack can make a machine or network crash, rendering it inaccessible to users. Malicious attackers may either provide the target with information that causes a shutdown or flood it with traffic to the extent that it crashes. Cybercriminals typically target cloud-based networks because they can typically be reached from the public internet. Hackers can initiate several cyberattacks following a successful one-on-one hit to target numerous others, as various organizations tend to share the same CSP. Furthermore, most malicious hackers are cognizant of and skilled at exploiting the knowledge that cloud-based systems tend to lack adequate protection. Any organization that loses essential data through malicious attacks, natural disasters destroying physical servers, or human mistakes can be significantly impacted. Backup and disaster recovery plans must be set up and reviewed to limit the potential loss. Security must be implemented on all levels of the network to limit the loss of data from cyberattacks.

Hacker interference and hacking: It goes without saying that when we refer to the cloud and its services, we're referring to the Internet as well. We also understand that the simplest way to communicate with the cloud is through an API. Therefore, protecting the APIs and interfaces used by external users is critical. However, cloud computing also offers a limited number of publicly available services, and those are its vulnerable areas since third parties can access them. Consequently, hackers might simply utilize those services to infect or hack our information.

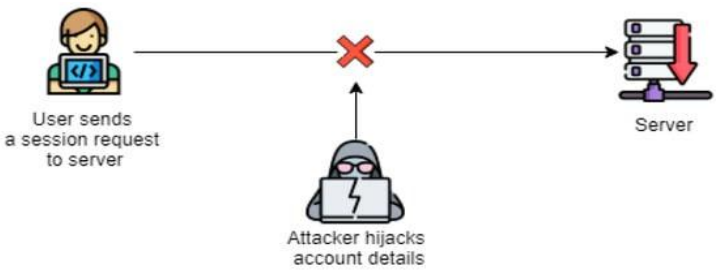

Fig.9.Interference of Hackers and Hacking

Data Loss: Data loss is one of the problems with cloud computing. This is often referred to as a "data leak." We are aware that we do not have complete control of our database and that an outsider might have access to our personal information. Thus, if the security of a cloud service is breached, hackers can gain access to our personal information or confidential data.

Lack of Skill: The primary issues in an IT firm with untrained employees are trouble in working, switching to another service provider, needing an extra feature, being able to operate a function, etc. Thus requires a trained individual to utilize cloud computing.

Multiple Cloud Management: In order to scale and provision resources, companies depend on various cloud environments. One of the issues with hybrid clouds is that most firms use a hybrid cloud model and have multiple clouds. The issue is that when more cloud providers are included, infrastructures become more complex and hard to manage, especially in the context of various technological constraints and differences in cloud computing.

An offline network can be the ransomware target, resulting in financial losses, damaging the brand of a business, and ruining relations with clients. Cloud security professionals must be knowledgeable about preventing and defending against denial-of-service attacks.

Phishing Attacks: Through the use of social engineering tactics, people or employees are persuaded to divulge private information like passwords.

Weak Passwords and Authentication: Some systems have insufficient authentication methods, and many users still use passwords that are simple to guess.

Third-Party Data Breaches: As third-party suppliers are frequently used by businesses, a breach can occur if these vendors don't have adequate security procedures.

Lack of Encryption: Without encryption, data is susceptible to eavesdropping and unwanted access.

Data Security and Privacy: Security of data is a concern of great magnitude while using cloud computing. Private and confidential user or company data is stored through cloud storage. Although the data service provider guarantees data integrity, you still remain responsible for user identification and authentication, identity management, encryption of data, and access control. Users lose confidence in your apps due to identity theft, malware infection, data breaches, and other cloud security issues. Employees or other individuals can intentionally or unintentionally compromise access to sensitive data.

Security system misconfiguration: First, it is hard for cybersecurity specialists to guarantee that only the right parties can access information since cloud architecture is designed for data exchange and availability. A prime example of this is link-based data exchange, where everyone with a link can access information.

Second, organizations that rely on the security setup of their cloud service provider (CSP) lose full visibility and control over their infrastructure.

The reality that most companies make use of multiple CSPs and have a difficult time getting familiar with the security regulations of each CSP is another cause of incorrect cloud security settings. Ineffective configurations and security blunders may stem from inadequate familiarity with all pertinent security procedures, creating loopholes that ill-natured hackers can exploit.

In order to resolve these problems, an amalgamation of technological remedies, user training, and adamant compliance with data privacy legislation and regulations is necessary.

Solutions For Data Security in Cloud Computing

Phishing Attacks:

- Notify users and employees regarding phishing emails so they can steer clear of clicking on suspicious links or downloading harmful attachments. Adopt email screening and authentication protocols to reduce the likelihood that inboxes receive phishing emails.

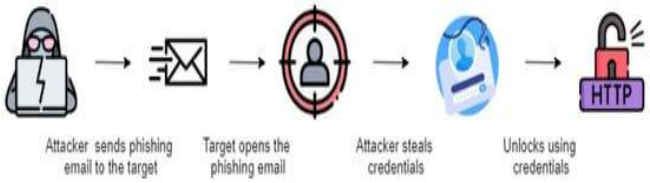

Fig.10. Phishing Attacks

Network Segmentation:

- Segment your network to prevent attackers from migrating laterally after gaining access to a specific area.

Frequent Software Updates and Patch Management:

- Ensure network hardware is configured to avoid security loopholes and install the latest software patches. Implement firewalls, antivirus software, and extra bandwidth for cloud data availability to reduce the risk of data security.
- To address known vulnerabilities, keep all software—including operating systems, applications, and firmware—up to date with security patches.

Access Control:

- Role-based access control (RBAC) can be implemented to limit access to sensitive information and systems.
- Implement the principle of least privilege (POLP) across all systems to ensure that users have access only as required for their tasks. To ensure that the terms and conditions, privacy policies, and compliance requirements of the platform provider align with your data protection requirements, you should also examine them.

User Education and Training:

- Educate staff members and users on how to spot phishing emails, social engineering schemes, and other online dangers.
- Employ cloud experts with expertise in DevOps and automation. Encourage your company's culture to be security-conscious.

Multi-Factor Authentication (MFA):

- Access control and authentication mechanisms are utilized to secure the privacy of information. MFA is applied to give an additional level of security when gaining access to critical accounts and environments. Companies need to establish interoperability and portability standards in the Cloud before initiating a project. The utilization of multi-layer permission and authentication methods for public, private, and hybrid cloud environments is also recommended for verifying accounts.

Encryption:

- It is advised that using encryption will protect records more securely. Data on a cloud server is easier to store until you encrypt the files. Data encryption should be used to safeguard users' privacy and the confidentiality of their data. Encrypt data to make it useless and to keep other people from obtaining it.
- Encrypt sensitive data while it's in transit and at rest to stop unwanted access. Make use of VPNs and encryption techniques such as TLS and HTTPS.
- An approach involving key sharing and authentication is suggested for maintaining data integrity and confidentiality. Robust key exchange and authentication protocols have the potential to enhance the security of the user-cloud services provider connection.

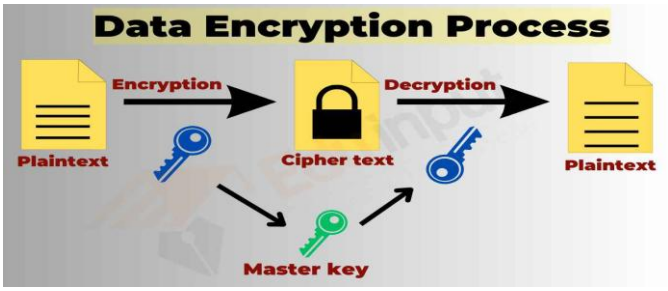

Fig.11.Encryption technology

Backup and Disaster Recovery:

- Regularly back up data and systems, storing backups offline, to protect against data loss in the case of a ransomware attack or other data breach. Formulate and evaluate a comprehensive disaster recovery plan.

Endpoint Security:

- Entry points utilised by malicious actors and campaigns to reach end-user devices such as desktop, laptops, and mobile devices. To protect specific devices, employ endpoint protection software (e.g., antivirus and anti-malware). Endpoint security systems protect these endpoint on a network or in the cloud from cyber threats. Administrators can log into their company's network with a centralized management console provided by endpoint security suites, which permits them to monitor, protect,investigate,and resolve problems with the network.

Incident Response Plan:

- The incident response plan is critical to a firm's overall cybersecurity framework as it ensures that security breaches are managed properly, minimizes potential damage, and accelerates the return to normal business operations. Establish an incident response team and define explicitly what role every individual will play. Develop an in-depth incident response plan specifying what will be done in the event of a cyber attack.

Security Audits and Penetration Testing:

- In security audits, there are two main types: internal, which focuses on in-house assessments, and external audits, which scrutinize from an outsider's perspective. Internal audits are primarily concerned with assessing and improving the efficacy of an organization's risk management, governance, and internal controls. External audits aim to provide an objective evaluation of an organization's financial statements and guarantee that they are accurate and compliant with applicable accounting standards and regulations. To find gaps and vulnerabilities in your systems and apps, conduct regular security audits and penetration tests.

Threat Intelligence:

- Follow threat intelligence sources to stay up to date on new threats and vulnerabilities.
- Make changes to your security plan in light of this information.

Zero Trust Security Model:

- Use a zero-trust strategy, which presupposes the possibility of threats both inside and outside the network. Regardless of location, verify and authenticate all access attempts.

Regular Security Awareness Training and Testing:

- Constantly instruct staff members and users on best practices for cybersecurity.
- Test their readiness by simulating phishing and social engineering attacks.

Continuous Monitoring and Incident Detection:

- Implement ongoing network traffic and system monitoring for indications of suspicious or malicious activities.
- Invest in SIEM (security information and event management) technologies.
- By conducting regular system audits and using resource-use monitoring tools, organizations can address this. It's among the greatest ways to control expenses and get beyond big challenges in cloud computing.

Strong password:

- Make use of a dependable password management system to safeguard all of your accounts. To bolster security, implement Multifactor Authentication(MFA) alongside a password for an added layer of protection tailored to your specific needs. Reputable cloud password managers keep users informed about security flaws and threats. The solution to password security issues may be as straightforward as implementing two-factor authentication. Make it a practice to update only the staff members who genuinely require access to the password security and to change the passwords as regularly as you can.

Cyber attacks and Hacking solution:

- Manage your social media settings.
- Get the right cyber insurance policy.
- Avoid saving password in your browser.
- Don't trust everything you read online.
- Verify that your system is current.
- Connect to the internet securely.
- Keep an eye out for phony emails and pop-ups.
- Keep your identity safe from theft.
- Control your social media preferences.
- Purchase the appropriate cyber insurance plan.
- Avoid saving passwords in your browser

IV.CONCLUSION:

The most reliable security solutions for cloud computing are provided. While cloud computing is a nascent, evolving technology that has numerous benefits for users, it also poses some security concerns. Working in a collaborative environment means sharing and securing data, particularly when dealing with sensitive or confidential information. Users can access cloud-based data and applications or devices securely with the appropriate cloud security solutions. Here, we've discussed some of the most important cloud computing data security concerns, their solutions, and a conclusion. Employing robust passwords and multi-factor authenticatication regularly backing up your data and checking your recovery plans, encrypting data, enforcing data retention and deletion policies, restricting and monitoring data access and permissions, and educating yourself.

V.REFERENCES:

[1].R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology, pp. 285– 295, Springer, Berlin, Germany, 2014.

[2].Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.

[3].R. Velumadhava Raoa,, K. Selvamanib, "Data Security Challenges and Its Solutions in Cloud Computing" in proceedings of the International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India .

[4].A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.

[5].S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[6].F. Zhang and H. Chen, "Security-Preserving Live Migration of Virtual Machines in the Cloud," J. Netw. Syst. Manag., pp. 562–587, 2012.

[7].J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[8].D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.

[9].E. Mohamed, "Enhanced data security model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12– 17, 2012.

[10]. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[11]. V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier.,2011.

[12]. F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.

[13]. Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013. [14]. L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez,"Building safe PaaS clouds: A survey on security in multitenant software platforms," Comput. Secur., vol.

31, no. 1, pp. 96–108, 2012.

[15]. A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, “Security risks and their management in cloud computing,” 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012 T. Mather, S. Kumaraswamy, and S. Latif, “Cloud Security and Privacy,” p. 299, 2009.

[16]. F. Yahya, V. Chang, J. Walters, and B. Wills, “Security Challenges in Cloud Storage,” pp. 1–6, 2014. [18]. Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM.

[17]. Lipinski, T. A. (2013, September). Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements. In International Symposium on Information Management in a Changing World (pp. 92- 111). Springer Berlin Heidelberg. Ransome, J. F., Rittinghouse, J. W., & Books24x7, I. 2009).

[18]. G. Atieniese, R. Di Puetro, L. V. Mancini and G. Tsudik. Scalable and Efficient Provable Data Possession. In Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, 2008, Art. 9.